Electronic Regulatory Filing Project

a joint project of the National Energy Board and the Ontario Energy Board

Issues and Comment

January 15, 1999

All National Energy Board and Ontario Energy Board publications are protected by the Canadian *Copyright Act*. This publication is not to be reproduced, in whole or in part, without the expressed permission of the National Energy Board and the Ontario Energy Board. For further information, please contact the Board Secretary at the following addresses:

National Energy Board
444 Seventh Avenue SW
Calgary, Alberta T2P OX8
(403) 292-4800
http://www.neb.gc.ca

Ontario Energy Board
2300 Yonge Street
P.O. Box 2319
Toronto, Ontario M4P 1E4
(416) 481-1967
http://www.oeb.gov.on.ca

101-00426/

CONTENTS

1. What is this report about? 1

2. What is the status of ERF? 1

3. What questions have been raised about ERF? 1

4. What is the legislative authority for ERF? 4

5. What criteria were used to design the ERF system? 6

6. How secure will the ERF system be? 7

7. What electronic formats will be used for ERF documents? 10

8. How will documents be signed in ERF? 12

9. Will ERF documents comply with the rules of evidence? 17

10. What will be the effect of ERF on confidential information filed with the Board? 21

11. How will ERF affect natural justice and procedural fairness? 21

12. How will documents be served in ERF? 23

13. Has the Board considered the effect of ERF on legal practice? 24

14. Does this mean that the Boards have answered every question about ERF? 25

15. Appendix A: Other Agencies and Jurisdictions 25

16. Appendix B: Selected Further Reading 30

17. Appendix C: Glossary 32

1. What is this report about?

The National Energy Board (NEB) and the Ontario Energy Board (OEB) are preparing to convert their information systems from paper to electronic form. Under the proposed Electronic Regulatory Filing system (ERF), all participants in the Boards' processes will deliver and receive regulatory information using computers. Paper documents will be the exception not the rule.

Note: This report has been prepared[1] to provide general background information pertaining to ERF. The legal discussion in it is of a general nature only and does not constitute legal advice. Readers seeking legal advice should consult their own advisors.

2. What is the status of ERF?

Beginning with a feasibility study completed in March 1993 , the Boards have proceeded carefully through cost benefit studies and progressive stages of analysis, design, and pilot implementation. During that time, regulated utilities, intervenors and others interested in the Boards' proceedings have participated in ERF workshops and planning sessions. A working prototype has already been demonstrated. Initial implementation is expected late in 1999.

3. What questions have been raised about ERF?

Two categories of questions include those that come from its relative novelty (like "How do I sign an electronic document?") and those that anticipate fundamental changes in the way the Boards operate (like "Will ERF lead to more written hearings?").

Questions of novelty will be resolved through training and familiarity. New technology invariably raises concern about risks. When photocopiers were introduced, for example, concerns were raised about accuracy of the reproduction. When fax machines were introduced, their use was scrutinized. Concerns were raised about the accuracy of fax copies, expense of faxing and the legality of facsimiles. Now both of these technologies, photocopying and faxing, are common, familiar and used almost without question, as are other familiar technologies like the telephone and television. That is, while there may still be problems with these technologies, most of the early concerns have been resolved not

---

[1] This report was written by Robin Nunn for the Ontario Energy Board and the National Energy Board (with special thanks to Stephen McCann, Charles Mathis and Claire McKinnon for their assistance).

through major changes in the technology but through better understanding of the technology and refining related processes.

Just as there are always concerns about potential risks in new technology, there is also a tendency to assume the opposite, that new machines, and in particular computers, are flawless. There is almost an expectation that if computers are not flawless then they are useless. Consider a common question: what is the possibility of losing track of a document among thousands of others in the computer system? This question is rarely asked about the present paper system. Everyone knows that paper can be lost. No practical computer system or paper system is without risk. Current systems used by the Boards, whether paper or electronic, are not flawless. A paper document may be misfiled or sent to a wrong address. The same errors can happen in a computer system. With proper design, however, errors may be tracked and corrected, whether the system is electronic or not. That is, risks of the proposed ERF system must be compared with the present system, not an abstract perfection that can never be achieved.

Between concerns about risk, on the one hand, and expectations of perfection, on the other hand, lies a middle-of-the-road issue: the danger of duplicating the present system with an electronic one. It may be possible instead, after examining the reasons for the present procedures, to adapt only necessary aspects to ERF. For example, handwritten signatures and affidavits are used now on documents filed with the Boards. Naturally there is a tendency to look for an electronic analogy such as a digital picture of a handwritten signature. Is this necessary? How is a picture, which can be duplicated by anyone, related to a handwritten signature that only the hand of the writer can make? Is a handwritten signature the only way to ensure that a document is "legal"? Are signatures examined and is forgery a likely event? These questions illustrate the opportunity both to avoid duplicating the present system and to design a better system. For more discussion of these specific questions, see the section in this report describing how documents will be signed in ERF.

Computers are impersonal. There is no human agent to act as a gatekeeper to information in a computer. The gatekeeper in a computer is a password or other technical device. Consequently there is a tendency to question how the impersonal machine will do all the things a person does to keep the system honest. Computers are also expected to measure up to their reputation for inhuman speed and efficiency. Consequently time becomes an issue where it may not be now. For example, users ask whether the computer system can be accessed twenty-four hours every day of the week. We do not ask this question about existing manual systems that are available only during normal business hours. Computers are expected to provide audited records and to confirm every step. In the present paper system, however, we often accept the risks of ordinary mail instead of registered mail. Computers also process huge amounts of information, yet the information is intangible and invisible until it is printed on a screen or paper. We implicitly trust a bound, typeset copy of a book because forgery would require skill and expense. Yet anyone can make words appear on a computer screen or printout. Who can say if they're genuine? For all of these

reasons, questions are raised about computers that would not be asked if the processes were more personal and tangible, less technical and complex.

Whatever the reasons for concern, and whatever system is eventually implemented, all parties must have confidence in it. Legal concerns may be raised merely as a means to establish whether the new ERF system should be trusted. Indeed, trust is one of the underlying themes in this report (see for example the discussion of trusted third parties and public key infrastructure). Paper is a trusted technology. Paper documents are used to establish the truth. Computer technology is new and not as trusted, and so invites a reconsideration of how trust and truth come to exist.

As noted above, there is a tendency when thinking about computers to have unattainable expectations. Some people may envision hearings in which the participants communicate only by tapping keyboards in a futuristic regulatory control centre where paper has been outlawed. Instead, ERF is intended to improve regulatory processes in specific ways that are focused not on technology but on structured and standardized documents:

- The core improvements are based on the information repository of electronic documents. Using an international standard called Standard Generalized Markup Language ("SGML"), all information in the repository will be in a formal, documented structure. The formal structure required to store documents (defined in a Document Type Definition, a "DTD") is expected to provide efficient document exchange and management. Information is expected to be more complete and easier to find and use.

- With information in a central repository, participants can select relevant parts of the information. This is expected to save the costs of distributing all information to all participants while providing requested information more efficiently. Documents can be pulled from the system, not pushed at everyone.

- Building on the core system, automated information management systems can facilitate meetings and hearings. This is known as the automated hearing room. In its simplest form, the automated hearing room will permit everyone present in the hearing room to search and retrieve documents electronically. This should not be confused with computer-aided transcription to produce verbatim hearing transcripts. Verbatim transcripts are only one type of document that will be stored in the ERF repository. Additional technology will permit participation from remote locations. Other possibilities include use of software for groups to work together at different times and places. This latter concept is called the electronic hearing room.

- Another proposed improvement is the use of case management and work flow tools to process documents and improve scheduling.

- The architects of the ERF system also propose to provide comprehensive help, not only about using the computer system but also about the substance of the regulatory process.

It is important not to confuse ERF with other technological innovations. It is not a computer-assisted transcript (CAT) system for instant verbatim reporting. It is not an electronic document interchange (EDI) system as used in commercial transactions for automated purchase and sale with standard purchase orders and invoices. ERF is not an imaging system that stores pictures of documents. These and other techniques can be part of the proposed system but they are not essential. The greatest benefits of ERF are expected to come from routine document creation and handling. Electronic documents can be automated and they do not need to be printed, duplicated, bound and delivered.

It is also important to distinguish an ERF document repository from a registration system. A land registry, for example, serves to register official documents. Documents are not accepted unless they fit in the prescribed format and only restricted types of documents are accepted. The information in a land registry directly affects legal rights. Contrast the registry model with the proposed ERF document information system that serves primarily to exchange information. Documents of many types are accepted so that participants can present their cases. Most documents filed with the Boards do not affect legal rights directly. Indeed, many documents are filed before a hearing begins and have no legal status until they are deemed to be admissible evidence. Even documents accepted as evidence do not usually have the force of registry documents that have direct legal consequences. These differences are strong influences in the design of the proposed ERF system (see also the discussion of other electronic systems).

The bottom line: ERF is a means of improving communication, not a change to the substance of the regulatory process.

4. What is the legislative authority for ERF?

When electronic documents were first encountered in legal proceedings, questions were raised about their status compared to paper records. In some instances, these questions have been resolved by legislation. For example, many statutes now give equal status to computer records and paper records (Access to Information Act, R.S.C. 1985, c. A-1, s.4(3), Canada Business Corporations Act, R.S.C. 1985, c. C-44, s. 22(1), Canada Evidence Act, R.S.C. c.C-5, s.30(12), Patent Act, R.S.C. 1985, c. P-4, s. 8(1)(1), Business Corporations Act, R.S.O. 1990, c. B.16, s. 139(1), Electronic Registration Act S.O. 1991 c. E.44, Land Titles Act, R.S.O 1990, c. L.5 , s.166(1), Registry Act, R.S.O

1990, c. R.20, s.16 (1) — see also the legislation in a growing number of American states that have followed the lead of Utah in passing statutes that say when corresponding with government, a digital signature is equal to a manual signature).

At the federal level, the Report of the Information Technology Security Strategy Steering Committee to the Council for Administrative Renewal, June 1995, made the following recommendations:

> "Although there is no legal impediment to the federal government using information technology, introducing the information technology security strategy, or implementing a public key infrastructure for digital signature and confidentiality encryption, the Steering Committee recommends *that legislation be reviewed, and possibly amended, in the following areas*:
>
> - The *Interpretation Act* and the *Canada Evidence Act* should be reviewed to clarify the evidentiary requirements for electronic records, particularly as they relate to statutory requirements for writing, original record, certified or notarized copy, etc.
>
> - Departments should review their own mandate and applicable statutes to ensure that the legislation provides for the use of these new information technologies.
>
> - The *Access to Information Act* and the *Privacy Act* should be reviewed to clarify requirements with regard to information technology, and in particular:
>
>   - computer searches and monitoring;
>   - smart cards;
>   - audit trails;
>   - central database and databases whose content changes frequently;
>   - formalities for exchanging information between government institutions.
>
> - Public key infrastructure legislation should be introduced to establish the many parties' roles and responsibilities, and to cap the federal government's financial liability. It is important that a lead Minister for such legislation be identified at an early stage.
>
> - The public should be consulted with regard to the issues of: the use of personal identifying information, for example, on government smart cards; the sharing of personal information among government departments, or between the federal and provincial governments, and; law enforcement access to encrypted information.
>
> - The legal responsibilities of operators of electronic bulletin boards and of persons who disseminate information on public electronic networks should be clarified.
>
> - Definitions of terms applicable in an electronic context is problematic, should be reviewed and possibly amended (eg. "private communications", "public place", "publication", "possession", "collection", and "disclosure")."

A proposed federal law, the Personal Information Protection and Electronic Documents Act (Bill C-54) would address some of these issues. Part 2 of Bill C-54 provides for

electronic alternatives to paper records governed by federal law. Instead of amending each individual federal statute, the Bill would amend the law generally. Federal government agencies will be authorized to use electronic means instead of paper, including electronic payments, forms and filings.

The NEB presently has the authority to make rules governing the conduct of its business (National Energy Board Act, R.S.C. 1985, C.N-7, s. 8). The National Energy Board Rules of Practice and Procedure, 1995 (SOR 95-208), refer explicitly to filing of documents. Section 9 authorizes filing in any form that the NEB has the facilities to receive. The same regulation, however, mandates filing of hard copy documents in addition to electronic filings. The rules are now being revised to accommodate electronic filings. The Ontario Energy Board also has authority over the conduct of its proceedings (Statutory Powers Procedure Act, R.S.O. 1990, c. S.22, s 25.1), and the information submitted to it (Ontario Energy Board Act, 1998, s. 13) and its rules too are being revised so that they will be neutral with respect to paper and electronic filings.

In the absence of more specific legislative provisions on electronic regulatory filing, general legal principles that evolved in a paper world must be reinterpreted for the electronic world.

5. **What criteria were used to design the ERF system?**

Early in the planning stages, a set of ERF principles and criteria was developed, including the following:

- Systems and processes which support the initiative must be effective, reliable and secure.
- Electronic documents must meet the following criteria:

  Electronic documents must have longevity, with documented information (including evidence) capable of being preserved over as long a time as appropriate for a court of record;

  Loading of documents into the system must be accurate;

  Loading of documents into the system (i.e. document repository) must be timely, and must require a minimum of handling;

  The presentation of a document (i.e. fonts and document layout) as intended by the author should, to the extent practicable, be preserved;

  Documents must be universally accessible, in other words, they must generally be retrievable and reusable regardless of the user's system or software that comply with open systems standards; and

  Exchange of documents should be possible using a variety of communication vehicles (e.g., E-mail, diskettes, Internet, file transfer, CD-ROM).

- To the extent practicable, the initiative will be based on an open, non-proprietary systems policy and standards.
- Systems supporting the initiative must be user driven, addressing and balancing the needs of all ERF participants and the general public.
- The systems and processes which support the initiative must enable long-term reductions in regulatory costs and process times.
- Where interim services are provided they must be cost effective in their own right and must contribute toward reaching the long term objective of ERF.

6. **How secure will the ERF system be?**

All computer systems require security measures. What kind of security is required and how much? The answer depends on subsidiary questions, including who has physical access to the computers and communication networks, who has electronic access, what are the incentives for someone to breach the security, what kinds of security breaches can be detected, what are the consequences of security breaches, what are the costs of protection, how secure is the present paper system in comparison, do security precautions interfere with normal use of the system and many other detailed questions.

The following topics must be addressed in any computer system:

- Authorization: authority to use the system (including not only authorized people but also authorized computers, that is, other computer systems that may also access the system)
- Authenticity: whether the users really are who they purport to be and whether the information they provide is what it is supposed to be
- Availability: whether the system is available and accessible when required
- Audit
- Confidentiality
- Integrity of information in the system
- Privacy

As noted earlier, no system is perfect. Current paper-based systems are not perfectly secure. Yet they have been deemed to be acceptable. Even locked filing cabinets behind locked doors can be breached by a determined intruder. Fire and water can damage any

records, whether paper or electronic. Abuse of an organization's information system may come not only from someone enabled by technology, such as the fabled computer hacker, but also from someone able to disrupt any system, such as a disgruntled employee. There is always a risk assessment, not an absolute guarantee of security.

Using reasonable computer security techniques, the proposed ERF system can be more secure than the present system. At present:

- Paper can be sent to the wrong address or be lost in the mail.
- Members of the public are permitted to handle original documents on the public record, which is therefore subject to damage, alteration or loss.
- Existing records may be incomplete.
- Old records may be difficult to retrieve.
- Present paper records are subject to error.
- There is no duplicate or backup system analogous to that provided by an electronic system for use after a disaster or during routine interruptions such as moving to a new location.
- Even documents given special status, such as signed affidavits, are not particularly secure now. It would be unusual for a tribunal to confirm the identity or authority of the person signing or to compare signatures on the affidavit with any other identifying document such as a driver's licence or passport.

Just as paper systems raise particular security issues (access to rooms, combination locks, keys) computer systems have their own issues (passwords, backups, power failure). A reasonably-constructed computer system will have as much as or more security than a paper system. As all documents will be electronic, identical copies can be provided as needed. Access to records can be controlled and audited. Computer verification techniques can reduce errors. Standard formats can improve data gathering and retrieval. Automation can minimize human errors.

Because computer systems can be made more secure than paper systems, computer security is often not a matter of whether the system is secure but how to balance security against ease of use. Too much security can be as inefficient as too little security. For example, a computer system could be made very secure if each document were given a unique password and a unique program for accessing that document. An intruder would have to know ten passwords and how to run ten programs to read ten documents. It is technically easy to create this kind of barrier. Unfortunately, legitimate users would also

face the same barrier. Nobody would want to use such a secure but inefficient system. Indeed, legitimate users would probably forget many of the passwords, or write them on paper and so create a new security problem in protecting the list of passwords.

Paper documents are so familiar that we rarely ask what are the required security elements. What gives us confidence in them? The same elements apply to digital documents. They include:

- authentication of the person— a document should show who signed it.
- authentication of the document— a document should show what the person signed.

Consider an ordinary letter signed by the letter writer. Many aspects of the letter could be used to prove it: a handwriting expert could testify about the signature, a materials expert could study the paper and ink, while the address, return address, postmark, stamp and the contents could all add to the ultimate confidence held in the document. Each of these elements, however, could also be forged. Handwriting can fool even an expert, or merely be illegible. Witnesses can lie.

In a computer system, authentication techniques should be designed to prevent forgery. The system should ensure that the person signing the document cannot deny doing so. Any commonly used technique should be efficient. Like a handwritten signature, it should be easy to do. Many of the techniques used in paper systems can be applied to computers, including acknowledgment of receipt (as in registered mail) and auditing of message traffic (mail tracking and logging).

Are electronic documents secure? Although no final decision has been made on the specific security programs to be used in ERF, the design of the proposed electronic document system includes provisions for software that will prevent unauthorized changes to documents. The system will be able to detect whether any information was changed, when the document was last changed and by whom. In this respect, paper documents which are easily changed are less secure than electronic documents under the proposed ERF system.

Are electronic documents vulnerable to forgery? In regulatory proceedings, forgery of documents is unlikely. The Secretary of the Board does not now examine the handwritten signature of the lawyer or witness filing a paper document to be sure it is a proper signature. An electronic document, by contrast, may have a secure code (digital signature, discussed elsewhere in this report) that serves the purpose of a handwritten signature.

An electronic system should also be able to ensure that the person sending a document cannot deny sending it and a person receiving a document cannot deny receiving it. Again,

the proposed ERF system makes provision for non-repudiation and auditing of transactions.

Authentication of a document is closely tied to verification of the contents. The techniques for signing documents should provide some means to verify not only what the signature attaches to but also that the signed document is complete and unaltered.

In some computer systems, even the security measures that protect the system are confidential and the location or perhaps even the existence of the computer systems is secret. A local example is the large unmarked suburban building that houses the computer systems of a major multinational company. There is no name on the building, just a street address. Any organization, even with such tight security, must be prepared to disclose necessary details about the computer system if required to prove computer records in court (see also the discussion of computer evidence).

Many organizations rely on the same computer security techniques including banks and law enforcement agencies which also need secure systems.

7. What electronic formats will be used for ERF documents?

In preference to proprietary formats, ERF uses open, international standards where possible. Consequently ERF does not accept formats specific to products like Microsoft Word or Corel WordPerfect. As the bulk of filings are text (that is, including words, tables, graphics and so on), the underlying architecture relies on the international standard text markup language, SGML. It is expected that XML and HTML will also be used to distribute information, although documents accepted in the repository must be in SGML. Some filings, such as high volume numerical data, may be stored in common relational database formats. Although document images produced by optical scanning or direct faxing may be used in exceptional circumstances, the architecture of ERF relies on searchable character formats. (See also the glossary in Appendix C for help with technical terms in this section).

There is no perfect document format. Nor is there a perfect way to search for information in a large repository. The Boards chose a format that permits contextual information to be encoded in the document itself. Such extra information, beyond the actual words in the document, can be used to search for documents, convert between formats or do other processing based on the extra intelligence encoded in the document. SGML permits individual documents to be used like databases, not merely stored.

Other formats can be searched word by word, but the familiar full-text search is subject to problems of noise and related concepts from basic information theory. Simply stated, when searching through a large repository, you get too much or too little information but

rarely the exact information required. Transcripts of testimony, for example, are difficult to search word by word given all the subtleties of human language. A witness may speak at length about "it", for example, describing it in great detail, with only indirect reference many pages earlier to what "it" is. Keywords that appear frequently in an energy database, like "natural gas", become no more useful in finding relevant passages than words like "it". Many document formats can be separately indexed to improve searching but that index is not contained within the document format itself. Even keyword indexing has its drawbacks, especially if indexed mechanically. By contrast, an SGML document can be indexed as it is created, with the desired elements and attributes embedded in the document by the author.

Formats that meld appearance and content, such as word processing formats and Adobe Portable Document Format (PDF), were designed to make text and graphics look good on a page. They attempt to reproduce an electronic version of paper. But the formatting will be distorted if the rendering device, usually paper or screen, cannot reproduce the typeface and other features used by the creator of the document. They are also substantially larger than SGML documents, and consume more communication and storage resources. A corollary of the separation of form and content gained by use of SGML is increased reusability of documents– converting between SGML documents or from SGML to other formats such as PDF is much easier than converting from a format with less embedded intelligence.

SGML is a mature international standard unlike proprietary formats that change frequently. The Boards have observed the problems experienced by other tribunals plagued by so-called upgrades. For example, when a new version of the approved word processing software appears on the market, the rules of the tribunal and the computer systems of all participants may have to be altered to process the new format.

SGML is complex and that complexity increases the costs of analysis, design, development and maintenance. The initial cost of an SGML system may be significantly higher than one based on proprietary formats, in part for DTD (Document Type Definition) development, and SGML may require additional software tools to support its use, but SGML documents are independent of the software that created them. The tools may be common to no-one, but the documents at the heart of the system are available to everyone now and in the future regardless of the proprietary tools used by any specific participants. Moreover, SGML tools have been rapidly increasing in power and decreasing in cost.

HTML, although simple and portable, is not extensible and cannot adapt to specific content. Consequently, as discussed above, the ability to search a large document repository for a specific HTML document is limited. Other limitations: HTML can handle only simple fill-in-the-blank forms and one-way hypertext links. Although each new version of HTML adds more capability, software changes to incorporate new versions consume time and resources. In any event, all versions of HTML mix format and content in a one-size-fits all document type definition.

In contrast to HTML, XML offers many of the advantages of SGML. Again without describing these markup languages in detail, some reasons to prefer XML over HTML include separation of content from format, opportunity to use various style sheets, improved linking, freedom to define document types (DTDs) and growing industry support for XML. Because XML is simpler than SGML, XML software development will be correspondingly simpler.

Despite growing interest in XML as a replacement for HTML, the ultimate power to formalize document structure resides in SGML. As SGML is the metalanguage underlying these other formats, support for SGML implicitly includes support for HTML and XML. The Boards' SGML implementation will be XML compliant. Other supported open formats include JPEG, MPEG and CGM for storing a variety of graphic and multi-media information without compromising archival requirements. Additional open standards will be supported as required.

8. **How will documents be signed in ERF?**

For centuries, various statutes have required that words be written, signed, certified, notarized or perhaps be fit into a prescribed form. These requirements help to prevent disputes about what exactly was said. A writing requirement, however, is not necessarily the same as a signature requirement. Writing can be unsigned. Writing captures ideas for many purposes, including use as evidence. Signatures identify and formally bind a person to the writing so that, in the absence of forgery, the person cannot disavow the writing.

Documents with legal significance are often signed in handwriting. It would seem natural, therefore, to demand that the electronic system have an electronic analogy to a handwritten signature. Before doing so, however, it should first be noted that a personally handwritten signature is not the only or even the most common means of investing a document with legal significance. A signature in the form of a handwritten name is not always needed. A mark, such as an 'X', intended to serve as a signature, may be acceptable. A stamp or facsimile may be acceptable, as is common on cheques and other commercial instruments. A signature created by a machine can be treated in law like a human signature. Judicial decisions in Canada, the UK and the US have held that mechanical stamps and other reproduced signatures are legally binding. Even an illegible signature has been accepted (see for example R. v. Kapoor (1989) 52 C.C.C. (3d) 41). In addition, the principal person involved need not sign the document. An agent can sign on behalf of a principal. A power of attorney can be used to delegate broad authority for signing. In government, legislation may delegate authority for signing.

The law has generally been flexible enough to adapt to new technology by accepting new forms of writing and signing or even by avoiding the requirements altogether. At both federal and provincial levels, statutory requirements for writing have long been interpreted to include various media, as expressed in terms such as these:

> "writing", or any term of like import, includes words printed, typewritten, painted, engraved, lithographed, photographed or represented or reproduced by any mode of representing or reproducing words in visible form." (Interpretation Act, R.S.C. 1985 c. I-21, s.2).

As noted elsewhere in this report, a definition such as this may be too restrictive for computer media, but it illustrates the flexibility of the concepts.

Specific laws have also been passed to eliminate writing and signing requirements. The federal government and some provinces have implemented the United Nations Convention on Contracts for the International Sale of Goods which provides that sale contracts do not have to be written. Ontario, for example, has removed a writing requirement from its Sale of Goods Act (R.S.O. 1990, c. S.1, see also the International Sale of Goods Act, R.S.O. 1990, c. I.10).

In a computer system, as in a paper system, handwritten signatures need not be the only means of authenticating documents. Depending on the circumstances, the effect of a signature may be achieved with electronic tagging like the addressing information on electronic mail, or by a typed name in the text of the message or by a facsimile of a signature in the form of a digitized image, or by processes requiring passwords and personal identification numbers. In some electronic filing systems, such as SEDAR (described elsewhere in this report), the filer must keep a manually signed piece of paper to support the electronic filing. Revenue Canada uses a similar technique with electronically filed tax returns. The filer, who keeps a handwritten signature of the taxpayer, acts as an agent of Revenue Canada to authenticate the tax return.

For the purposes of this discussion, none of the above forms is considered to be a digital signature. A digital signature is not a visual concept but rather is the result of mathematical calculation applied to the document. In other words, a digital signature uses a "secret code". The sender does not have to be a mathematician but merely needs software that does the appropriate calculation and attaches a signature to the document. The signature does not alter the contents of the document but rather is additional information. In some systems the code can be used to scramble (encrypt) the whole document to make it confidential, but document encryption is not a necessary part of a digital signature system. Whether the message itself is encrypted or not, a digital signature can nevertheless be used to determine if unauthorized changes have been made to the text of the message.

The concept of a digital signature is possibly confusing and certainly new for most people. For that reason it is discussed in this separate section although it is closely related to other issues like system security and admissibility of evidence.

To be effective, the signature code is calculated so that it identifies the signer, cannot be created by anyone but the signer and it can be verified by the recipient of the document.

Note that the recipient's software does not need the sender's secret code, called a private key, but only the corresponding public key used to check the signature.

Digital signature software usually relies on complex mathematical concepts such as the properties of prime numbers, hash functions and asymmetric cryptography, which are beyond the scope of this discussion. From the point of view of users of a digital signature system, a digital signature can be as simple as an added string of unintelligible characters at the bottom of an e-mail message. This string of characters is processed by the recipient's software to authenticate the signature and the message. The fundamental feature of a digital signature is that it can be traced to the person who made it. Only the person with the private key can make the signature. The non-mathematical forms of signatures listed above, such as a typed name or digital facsimile, cannot necessarily be traced because they can be reproduced by anyone.

More important than the mechanics are the fundamental reasons for using signatures. The purpose of a signature is to attest to the authenticity of a document. A signature provides evidence that the signer actively approved of the contents of the document and intended to be bound by the consequences. A valid signature cannot be repudiated by the signer. Any system, paper or electronic, must show who signed (signer authentication), what exactly was signed (document authentication) and do so efficiently so that the transaction cost of using signatures is minimal.

In regulatory proceedings generally, the signature on a document is not verified by the recipient of the document, although it is available if needed. Rather, the procedure by which the document is created and delivered to the recipient gives the document its authority. Pre-filed evidence, such as an economic forecast, for example, must be proved at a hearing. A signature on the forecast is of little value before a witness has attested to the document and has had an opportunity to explain, correct or update it.

Appropriate procedures can substitute for a handwritten signature. Familiar examples of procedure substituted for handwriting include:

- electronic home banking
- paying by credit card over the telephone
- online personal property security registrations
- purchase of securities from a broker

Each of these examples uses different safeguards to ensure that an authorized person or delegate is bound by the transaction despite the absence of a handwritten signature.

As there is currently no formal screening process at the Boards to detect fraud or forgery of signed documents, the proposed computer system cannot significantly increase the likelihood of fraud or forgery. Rather, the system can automate the process of verifying signatures. A general hardship provision can relieve a participant from the requirements of the system depending on the circumstances.

Together with digital signatures comes the need for a public key infrastructure (PKI) with trusted third parties or certifying authorities. A handwritten signature can be linked to a person by watching the person sign and by comparing handwriting samples. A digital signature is merely a stream of numbers. The digital signature can be linked to the person by having a third party keep records to verify that the stream of numbers has been issued to the person who claims to have that particular digital signature. That is, a third party can take responsibility for issuing and revoking digital signatures and generally monitoring the digital signature system.

Federal Bill C-54 (discussed elsewhere in this report) contemplates regulations deeming certain technologies to be acceptable for secure electronic signatures. Some of the issues that must be considered in making these regulations are stated in these terms:

> "The Governor in Council may prescribe a technology or process only if the Governor in Council is satisfied that it can be proved that
> (a) the electronic signature resulting from the use by a person of the technology or process is unique to the person;
> (b) the use of the technology or process by a person to incorporate, attach or associate the person's electronic signature to an electronic document is under the sole control of the person;
> (c) the technology or process can be used to identify the person using the technology or process; and
> (d) the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document." (s. 48(2)).

The proposed legislation also ties the concept of secure electronic signatures to the law of evidence in the following terms (see also the discussion of authentication):

> "The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting
> (a) the association of secure electronic signatures with persons;
> (b) the integrity of information contained in electronic documents signed with secure electronic signatures; and

(c) the manner in which the matters referred to in paragraphs (a) and (b) may be proved." (s. 31(4)).

Bill C-54 distinguishes secure signatures in general from the specific technology of digital signatures. Future secure signature technologies, such as transmission of biological data, may also be prescribed. Bill C-54 defines both "electronic signature" and "secure electronic signature", the latter requiring the application of prescribed technology. A secure electronic signature would also satisfy a legal requirement for a seal.

The proposed law permits electronic documents to satisfy a writing requirement under scheduled laws. If an original document is required by law, the electronic version would need a secure electronic signature. Statements made under oath or affirmation, such as affidavits, could be made electronically using two secure electronic signatures, one of the person swearing the statement and another of the person authorized to take the statement. Similarly, signatures that must be witnessed could be made with two secure electronic signatures, that of the signer and that of the witness.

If secure signatures are more secure than handwriting, we now have new categories of trust. In a paper world, we now use a signature and occasionally the extra protection of a witness. Under some laws the witness may be anyone. Other laws require an official witness, such as a commissioner for oaths or a notary public. The secure electronic signature offers a new kind of witness, the certifying authority. Some situations may still require the electronic equivalent of an affidavit, but in many situations only a single secure signature may suffice. For example, the presence of an impartial witness may be needed to confirm the mental state of the signer. Where, however, the impartial witness is only confirming that the document was signed without inquiring into the intentions of the signer, only a single secure signature may be needed. That is, the idea of a witness's digital signature raises the question: what does the second signature witness?

Systems for handling electronic signatures are complex. One of the most effective ways to move from paper to electronic documents, then, is to remove any unnecessary signature requirements. Board rules may have to be examined to be sure that signatures are not required merely because they have always been required. For example, signatures under oath, on affidavits and notarized documents, may be a means of attaching criminal penalties to false filings. The same purpose can be achieved by a general rule or regulation deeming use of the computer system to constitute signing, with penalties for any false filing, without demanding individual oaths for each document (see for example the Employment Insurance Regulations SOR/96-332, ss. 90, 91).

9. Will ERF documents comply with the rules of evidence?

The evidence on which the decision of a tribunal is based should be relevant and reliable. If evidence is not relevant, it cannot assist the decision maker. If evidence is not reliable, or if

there is no way to tell whether it is reliable, it cannot be used to establish the facts of the case. Irrelevant or unreliable evidence is either excluded from consideration altogether or admitted but not given any weight in the decision. The question for the proposed ERF system, then, is whether the system will provide relevant, reliable, admissible evidence.

Among the various categories of evidence used to prove a case— such as oral testimony, written evidence, real evidence and so on —the category most relevant to the proposed ERF system is documentary evidence. Before a document can be admitted as evidence and made an exhibit, it must pass several tests. For example, the document must be authenticated, that is, shown to be genuine. The so-called best evidence rule also requires the original document if it is available. These and other evidentiary rules have many exceptions. Very old documents, for example, are generally assumed to be authentic.

Computer records have been admissible in court as documentary evidence under common law principles. In addition, there is a specific statutory provision for documents, including computer records, made "in the usual and ordinary course of business" (Canada Evidence Act, R.S.C. c. C-5, s.30, Evidence Act, R.S.O 1990, c. E.23, s. 35).

The language of the Evidence Act does not specify how to ensure that computer records are admissible. Even if the records are admissible, there is no specific standard for ensuring that the records be given appropriate weight in the tribunal's deliberations. The courts will look at the overall circumstances of making the records. In general, admissibility and weight of computer records depends on reliable processes for input, storage and retrieval of the information:

> "The nature and quality of the evidence put before the Court has to reflect the facts of the complete record-keeping process— in the case of computer records, the procedures and processes relating to the input of entries, storage or information, and its retrieval and presentation" (*R. v. McMullen* (1979) 47 CCC (2d) 499 at 506, 25 OR (2d) 301, 100 DLR (3d) 671).

In other words, there is no way to *guarantee* that a specific computer record will be admissible and given appropriate weight. Of course, a regulatory tribunal is not a court of law subject to every nuance of evidence law.

In any event, the focus of inquiry in a dispute about the validity of ERF documents would not be on the particular piece of paper or record. The inquiry would be about the record-keeping system that produced the record. That is, the ERF system— the complete record-keeping process cited above —must be reliable and meet industry standards.

Although federal and provincial evidence law refers to computer records, it does not refer to finer distinctions such as the difference between imaging and optical character

recognition. Imaging systems copy documents without separating individual parts of the image into letters and numbers. Imaging is subject to errors during input of the image and in the finite capacity of digital systems. That is, images in the real world may contain more information than can be captured in a reasonable storage space in the digital world. Unlike imaging, optical character recognition tries to separate meaningful parts of the image but is subject to interpretation, such as whether a dot is punctuation or merely a stray speck on the image. Yet another form of computer record is made when a computer file is copied from one disk to another disk. Unless the copy is verified byte for byte, the copy cannot be assumed to be exact, although it usually is. These different ways of creating computer records are all subsumed under the heading of computer records. Yet they vary in their trustworthiness. The latter type of copy is verifiably exact but few users of optical character recognition would expect perfect text every time. Imaging lies somewhere in the middle of the trustworthiness scale depending on the quality of the original paper documents, the sophistication of the imaging equipment, the imaging algorithms used (e.g. lossless or lossy compression) and the size and format of the stored images. (In this regard it is noteworthy that Revenue Canada issued an information circular for the purpose of including imaging as a method of keeping tax records. See Information Circular 78-10R2SR, February 10, 1995 which requires that records be kept according to standards set by the Canadian General Standards Board in Microfilm and Electronic Images as Documentary Evidence, (CAN/CGSB - 72.11-93)).

In regard to copies, there is no way to be sure what a court would say about destruction of original records used to make computer records. If destruction is the ordinary course of business, then the records might pass that test. If not, destruction might be deemed to be obstruction and deception (see also the discussion of professional practice issues). The Evidence Act has special provisions for destruction of signed documents that have been photographed (i.e. microfilmed) but does not specifically include digital documents (Canada Evidence Act, R.S.C. 1985, c.C-5, s.31, Evidence Act, R.S.O 1990, c. E.23, s.34).

Other evidentiary principles may apply in addition to the "ordinary course of business" discussed above. Underlying all of evidence law is the need to put accurate facts before the tribunal. To meet this need, courts prefer:

- records made contemporaneously with the events they describe (because human memory fades)
- records made from personal knowledge (not potentially unreliable hearsay)
- facts not opinions (the familiar "just the facts, please", leaving opinions for experts and the tribunal)
- original records not copies (a principle developed in a paper world where copies are not identical to originals)

- records made routinely and because the maker had a duty to do so (not records concocted for self-serving purposes)

These apparently simple standards often cannot be met by computer systems. As described previously, computers are impersonal. Records are often maintained and manipulated by someone who has no knowledge of the making of the records. Records may be retrieved much later than the events recorded. Records in a computer system can be an amalgamation of information made within an organization and information from other computer systems outside the control, knowledge or accountability of any one person. Facts in a computer can be part of a system of software used to manipulate the facts, as in a spreadsheet that can produce countless variations from the same data. It is clear that the law of evidence will have to evolve to deal with electronic record-keeping.

The Uniform Law Conference of Canada has recently approved a Draft Electronic Evidence Act and Commentary. That document addresses numerous evidentiary issues such as authentication, the best evidence rule and standard procedures. For further information see http://www.law.ualberta.ca/alri/ulc/current/eueaa.htm.

Under federal Bill C-54, discussed elsewhere in this report, scheduled federal laws that require copies would be satisfied by a single electronic document. Bill C-54 deals with the issues of original documents by deeming electronic documents to be satisfactory if "the electronic document contains a secure electronic signature that was added when the electronic document was first generated in its final form and that can be used to verify that the electronic document has not been changed since that time." This language is open to various interpretations, including what constitutes "first" generation and "final form", with all the possible versions in between.

Evidentiary issues of authentication and best evidence are considered in Bill C-54 in these terms:

> "31.2 (1)The best evidence rule in respect of an electronic document is satisfied
> (a) on proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored; or
> (b) if an evidentiary presumption established under section 31.4 applies.
> (2) Despite subsection (1), an electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout.
> 31.3 For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven
> (a) by evidence that supports a finding that at all material times the computer system or other similar device used by the electronic documents system was

operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;
(b) if it is established that the electronic document was recorded or stored by a party who is adverse in interest to the party seeking to introduce it; or
(c) if it is established that the electronic document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce it."
31.4 The Governor in Council may make regulations establishing evidentiary presumptions in relation to electronic documents signed with secure electronic signatures, including regulations respecting
(a) the association of secure electronic signatures with persons;
(b) the integrity of information contained in electronic documents signed with secure electronic signatures; and
(c) the manner in which the matters referred to in paragraphs (a) and (b) may be proved.
31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document."

The juxtaposition of evidence law and computers raises many questions. As more government institutions entrust their business records to computers, the issues discussed in this section will be resolved. Meanwhile the ERF system is being designed with these questions, including the unanswered ones, in mind.

10. What will be the effect of ERF on confidential information filed with the Board?

Confidential business information may be supplied to the Board (such as that specified in section 16.1 of the National Energy Board Act or part VII of the Ontario Energy Board Act, 1998). Other principles of general application, such as fiduciary duties, may also apply as they do now. The proposed ERF system is not expected to have any effect on confidentiality. Differences between the existing paper system and the proposed ERF system are primarily related to computer security compared to existing security, discussed elsewhere in this report.

11. How will ERF affect natural justice and procedural fairness?

The concepts of natural justice and procedural fairness are intended to ensure that affected parties know the case to be heard and can present their evidence and argument before an impartial tribunal. The specific procedural standards that will achieve these ends depend on many factors including the kind of tribunal and the effect of the decision. Courts have analyzed fairness and natural justice not as necessary requirements for every tribunal but as appropriate for the circumstances. Different tribunals do different things, from court-like determinations of individual rights on the one hand to broader policy decisions on the other hand. Less strict procedural requirements are applied to policy matters. Many lengthy treatises have been written on these concepts which will not be further defined here.

To the extent that ERF is simply automation of document creation, transmission, storage and retrieval, it should have no effect on procedural standards. In other words, the Boards will continue to have hearings, make decisions and so on. There are several aspects of ERF, however, that deserve specific comments.

The first is the question of fairness to individuals, small intervenor groups and those who do not now use computers. Will a system dependent on use of computers exclude anyone? No.

Most participants in the Boards' processes are represented by lawyers who have access to computers. A survey of participants showed that they are using various types of computer systems. The survey was completed early in the planning stages of ERF and undoubtedly would show even more technical sophistication today. There are also unrepresented intervenors, primarily concerned with issues such as construction on the intervenor's land, and a larger number of unrepresented individuals who do not intervene but who present their views through letters of comment.

Anyone who participates in proceedings under the present system must be able to read either official language, comply with Board rules and communicate by mail, fax or by attending personally. These requirements are not perceived to be unfair. In the proposed system, these requirements change little. Paper documents can be converted to electronic form compatible with Board standards. Even if an individual has only a pen and paper or a typewriter, the individual can submit the paper and the ERF system can store a digital version of it.

Conversely, to assist the public in getting documents from the system, computer access will be made available for online searching. Does this exclude members of the public who do not know how to search for documents in the computer system? Again, the baseline for comparison is the present system. Do members of the public know how to find documents in the present system? They must take the time to understand the rules, the process and the paper documents. Progress reports and studies of the proposed ERF system suggest

that document retrieval will be greatly improved under ERF. Moreover, the tribunal has the power to regulate its procedure and in particular to require that information be filed with indexes, executive summaries, cross-references and other techniques that can reduce the complexity of even the largest cases.

A related question is whether the use of computer technology will make the Boards more remote from the public. Computers are no longer specialized tools for experts— not in an era when public school children use the Internet in their classrooms, when telephone and cable companies make e-mail as available as telephones and televisions, and when many government agencies advertise their world-wide web sites. In many ways the proposed ERF system will make the Boards less remote: access to information will be improved not only through automated searching but also with more uniform filing and keyword tagging. ERF can also provide forms of access not available now for the disabled, including off-site computing, large-font display, Braille and speech synthesis. ERF will literally make the Boards less remote to participants in remote areas.

Indeed, electronic access may open the Boards to new audiences. An electronic document repository may provide public information to anyone with an Internet connection. The public record has always been open to the public, but only at Board offices. Instantly accessible and searchable public information is a new phenomenon, perhaps even a new category of public information.

Existing rules of practice and procedure may have to be revised to accommodate ERF. The rules now assume a paper world. For example, words like "original" and "copy" will have to be revisited in the context of electronic filings. Rules, guidelines and procedures will, of course, have to take into consideration the rights and needs of participants who do not own a computer or whose ability to use one is limited. The Boards will provide access to everyone as required whether by means of computers or traditional paper processes. Anyone without access to a computer will be accommodated.

One issue that merits special attention is that of notice. Natural justice and procedural fairness require that potential parties have notice of Board proceedings. Failure to give reasonable notice may invalidate a decision. Notice need not be personal delivery of a piece of paper (see also the discussion elsewhere in this report of document service generally). On the contrary, because so many parties may be interested, notice of Board proceedings is typically published in newspapers. No Canadian court has ruled on use of an Internet site or e-mail for public notice of proceedings. By analogy to existing rulings, however, it is likely that a court will inquire whether electronic means of notice are reasonable in the circumstances. Until the Internet and computer technology become as broadly and routinely consulted as the daily newspaper, however, the Boards will continue to give notice using traditional means in addition to any electronic means.

12. How will documents be served in ERF?

Today most documents are created electronically with word processing software, or other applications such as spreadsheet and e-mail software. They are then printed, filed and served as paper among the parties to the proceeding. Some parties may then scan the paper back into an electronic form for easier storage, searching and retrieval. The ERF document repository can eliminate some of these conversions and permit documents to be pulled from the system as required.

In a paper system, documents are not only filed with the tribunal but they are also served on interested parties. Filing and service ensure that parties know that documents exist and have access to them. Parties also cannot say they were unaware of the existence of the filed documents. This is an example of document "push" in which all documents are always delivered to all parties, regardless of their particular interests in the proceeding.

In an electronic system, automation makes it possible to provide different types of service, or eliminate service entirely. Parties could sift information according to their own interest profiles. They could receive documents by e-mail. Or rather than receive whole documents, they could simply receive notification that certain documents had been filed. Then they could pull documents from the repository as required. Or they could dispense with service altogether and check the repository for new documents, either manually or using an automated software agent for periodic updates.

No Canadian court has ruled on the legality of digital document service or eliminating service altogether in favour of document pull. Considering judicial decisions about technologies such as fax and telegraph, a court would be likely to look at the particular technology and the circumstances. In any event, the Boards have the power to control their own process, are not bound by the procedural requirements of courts and have prescribed their own filing and service requirements (National Energy Board Rules of Practice and Procedure, 1995, SOR/95-208, ss. 8 and 9, Ontario Energy Board Rules of Practice and Procedure, February 1997, ss. 11 and 20).

If, as in the present paper system, parties know about all filed documents and have access to them, with appropriate safeguards such as acknowledgment messages, then the objectives of document service could be achieved electronically. Although no final specification has been developed, the ERF system is being designed to meet these objectives.

13. **Has the Board considered the effect of ERF on legal practice?**

Consider these statements from lawyers published in the Ontario Lawyers Gazette, February 1997, by the Law Society of Upper Canada, the governing body for Ontario lawyers:

> "Law is very conservative . . . we're not going to be the first ones to test whether an electronic document is admissible in court."
>
> "It's like dragging the past in, but I'm not comfortable going to that fully electronic world if my career is going to turn on whether that fax I send from my computer really went out."

Law practice issues include whether instructions from clients must be signed on paper. Would e-mail instructions suffice? If so, how long should old e-mail be kept? Some lawyers may believe that only paper records will protect them against claims for errors and omissions and that all records must be kept forever. Issues like this between lawyers and their clients are not generally brought before a regulatory tribunal. Still, lawyers such as those quoted above may believe that they must exchange paper, not electrons, "out of an abundance of caution."

By the time ERF is fully implemented, it is expected that lawyers will be using computers in other areas of their practice and will have policies for electronic records and filing. In the meantime, any implementation of ERF will have to take some account of lawyers' professional responsibilities in relation to record-keeping.

14. **Does this mean that the Boards have answered every question about ERF?**

No. ERF is new. Until it has been implemented and tested, there will naturally be questions and problems to resolve. As noted at the outset, many questions will be resolved through familiarity with the new technology, which will only be gained over time. If there are unresolved questions, the Boards welcome comments and suggestions.

15. Appendix A: Other Agencies and Jurisdictions

Although ERF and its associated issues are new in Canadian energy regulation, the Boards are not alone. Other agencies and jurisdictions are also converting paper to electronic systems.

Canadian Federal Examples

The government of Canada has too many electronic programs to list here (see for example the list at http://www.gc.ca/programs/pgrind_e.html). They include:

CANADIAN ENVIRONMENTAL ASSESSMENT AGENCY (CEAA)

The Canadian Environmental Assessment Agency, pursuant to section 55 of the Canadian Environmental Assessment Act, operates a public registry system. The purpose of the registry is to facilitate public access to the records relating to environmental assessments, and to ensure convenient public access. The public registry includes the Federal Environmental Assessment Index (FEAI), departmental document listings and documents.

THE CANADIAN INTELLECTUAL PROPERTY OFFICE (CIPO)

The Canadian Intellectual Property Office permits online searching of the Canadian Patent Database. From the online description:

> "This database lets you access over 75 years of patent descriptions and images. You can search, retrieve and study more than 1,300,000 patent documents."

CIPO also offers the Canadian Trademarks Database, described online as:

> "enabling you to look up all pending and registered trade-marks in Canada. Trademark information found in the database can include designs, wares and services covered by the registration, owner's name and more."

DIGITAL SIGNATURES

The federal government is already using digital signature technology, as in the novel application described in these words:

> "On June 5, 1998, the Communications Minister of Singapore, Mah Bow Tan, used a digital signature to sign a Memorandum of Understanding between his country, Canada, and the State of Pennsylvania. The signing took place at an Asia-Pacific Economic Cooperation (APEC) Meeting on the Telecommunications and Information Industry. Canadian Minister of Industry John Manley and Pennsylvania Governor Tom Ridge, neither of whom was present at the meeting,

had both previously signed the document using private key technology. The signatures were delivered ceremonially to Minister Mah at the meeting by representatives. Minister Mah then placed a smart card containing his signature into a reader, and typed in his password to "sign" the document. The three signatures were then electronically authenticated to create an offical document. The document is the first digitally signed international government document and it creates a Global Learning Consortium between the two countries and the state to promote the use of telecommunications and information technology in education through a common website." (http://www.tas.gov.sq).

Examples from Ontario

In Ontario, examples of pioneering electronic systems include: personal property security registration, business names registration, land titles and land registry, civil trial procedure and securities commission filings.

MINISTRY OF THE ATTORNEY GENERAL, ONTARIO

A pilot project authorized under the Courts of Justice Act (O.Reg 223-97) permits lawyers to file a limited number of civil court documents electronically. Electronic filing is part of a larger civil case management project using proprietary software called Sustain to enter claims, schedule cases and produce statistical reports. Only designated law firms and legal departments trained in the use of the prescribed software may participate. In the pilot project, a lawyer uses Sustain client software to create and then e-mail a one-page word processing template to the court office. The software verifies the form, debits the filing fee directly from the lawyer's account, issues a court file number and sends a receipt to the lawyer. Service of documents between participating solicitors may be done through the computer system. The prescribed forms do not require a signature, although a signed proof of service must be kept by the lawyer. Public access to filed documents will initially be available at terminals in the court and later by remote access, and paper copies will also be made as required. Long term plans not part of the pilot project include filing of motions and trial records in addition to simple one-page documents.

The Sustain system, unlike ERF, uses proprietary software and data formats. A consortium of companies including Microsoft promotes the software as an electronic way to link lawyers and courts. The Ministry project is also associated with a separate administrative court management process.

MINISTRY OF CONSUMER AND COMMERCIAL RELATIONS (MCCR)

In partnership with a private company, Teranet, MCCR has developed an electronic land conveyancing system. MCCR also has an electronic system for filing personal property security registrations and one for business name registration. More than 90% of personal property registrations and 30% of business name registrations in Ontario are filed electronically. These systems use proprietary software and data formats. In most cases, only designated persons may participate. Under the regulations governing these systems, documents do not have to be signed. Unlike ERF, the registries are not primarily for document management in hearings and adjudication.

Cross-Canada Example

CANADIAN SECURITIES ADMINISTRATORS (CSA)

Canadian securities regulatory authorities have adopted an electronic filing system, the System for Electronic Document Analysis and Retrieval (SEDAR). SEDAR was developed to:

> "Facilitate the electronic filing of securities information prospectuses, continuing disclosures documents, etc.) and the payment of CSA filing fees as required by the securities regulatory authorities in Canada.
>
> Facilitate public dissemination of securities information collected in the securities filing process.
>
> Facilitate electronic communication such as E-mail between electronic filers, filing agents and securities regulatory authorities."
> (SEDAR Filer Manual)

Unless there are exceptional circumstances, all filed documents must now be in electronic form. Unlike the proposed ERF system, SEDAR does not use the standard generalized markup language, SGML. All SEDAR documents must be in one of three proprietary formats (WordPerfect, Microsoft Word, Adobe PDF).

Examples from the United States

RULENET

An innovative experiment by the U.S. Nuclear Regulatory Commission (NRC), RuleNet was an electronic rulemaking forum on the Internet. The experiment involved the public in making performance-based rules related to fire protection. Anyone with a Web browser could observe, post comments and access related documents.
(http://nssc.llnl.gov/RuleNet/Help/Info.html)

FEDERAL COMMUNICATIONS COMMISSION (FCC)

In April 1997, the FCC started its electronic filing initiative with a Notice of Proposed Rulemaking (FCC 97-113):

> "In this Notice of Proposed Rulemaking (Notice), we propose to allow parties to file comments electronically in all FCC informal notice and comment rulemaking proceedings conducted under section 553 of the Administrative Procedure Act, except for broadcast allotment proceedings. These electronic filings would be given the same treatment and consideration as comments filed on paper. We tentatively conclude that this action will make it significantly easier for members of the public to communicate their views to the Commission, and to review comments that others have filed. We believe that electronic filing will also allow the Commission to improve the efficiency of its own processes, to the benefit of the public."

OTHER AGENCIES USING SGML

The following is a list from the SGML Web Page (http://www.oasis-open.org/cover/ as of November 1998) of government and industry SGML projects:

- The U.S. Department of Energy (DOE) Office of Scientific and Technical Information (OSTI)
- IRS (United States Internal Revenue Service)
- National Library of Medicine (NLM)
- Library of Congress - Encoded Archival Description (EAD) - Finding Aid Pilot Project
- SAE J2008 (and T2008) Automotive and Truck Standard
- SEC EDGAR Database
- IETM (Interactive Electronic Technical Manuals)
- TCIF/IPI (Telecommunications Industry Forum Information Products Interchange)
- Electronic Component Information Exchange (ECIX) - Pinnacles Component Information Standard (PCIS)
- ATA DTDs (Air Transport Association)

- Railroad Industry Forum: Electronic Parts Catalog Exchange Standard (EPCES)

- CALS: Continuous Acquisition and Lifecycle Support (formerly: Computer-aided Acquisition and Logistics Support; recently "Commerce At Light Speed")

- USAF SGML Repository

- MIL-STD-2167A: FOSIs and DTDs related to MIL-STD-2167A

- MIL-M-28001B SGML documents (Navy site)

- Army SGML Registry and Library (ASRL)

- Government Information Finder Technology - GIFT (Canada)

16. Appendix B: Selected Further Reading

Aspects of Public Policy Regarding Crown Copyright in the Digital Age, W.T. Stanbury, 10 Intellectual Property Journal 131, May 1996

Copyright and Confidential Information Law of Canada, G. F. Henderson ed, 1995 Carswell

Copyright and the State in Canada and the United States, David Vaver, 10 Intellectual Property Reports 187, May 1996

Copyright in Legal Documents, David Vaver, 1993 Osgoode Hall Law Journal Vol. 31 no. 4 p. 662

Crown Copyright In Canada: A Legacy Of Confusion, Barry Torno, 1981 Minister of Supply and Services Canada

Essentials of EDI Law, Peter Jones, Electronic Data Interchange Council of Canada, 1992

The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet", Stephen M. Johnson, Administrative Law Review, 50:2, Spring 1998, p.277ff;

Management of Recorded Information, Directive 7-5-8 June 1992, Management Board of Cabinet, Ontario

Microfilm and Electronic Images as Documentary Evidence, CAN/CGSB - 72.11-93, Canadian General Standards Board

Ontario Lawyers Gazette, January/February 1997, Vol. 1 No. 1, Law Society of Upper Canada

Open Access Same-Time Information System, 18 CFR Part 37 April 24, 1996 Federal Energy Regulatory Commission (FERC)

Policy, Practice and Who Gets to Own the Crown's Jewels: The Ownership of Intellectual Property in Crown Contracts, Martin P. J. Kratz, 10 C.I.P.R. 613

Practitioner's Guide to Electronic Filing in Utah Courts, April 27, 1995, Utah Administrative Office of the Courts

Recorded Information Fact Sheet # 6 on Electronic Document Filing Fundamentals, Archives of Ontario

Report of the Information Technology Security Strategy (ITSS) Steering Committee to the Council for Administrative Renewal, June 1995 (http://www.cse.dnd.ca/GOCITSTRATEGY/).

Revenue Canada Information Circular 78-10R2SR, February 10, 1995

SEDAR (System for Electronic Document Analysis and Retrieval) The Ontario Securities Commission OSC Bulletin November 15, 1996 Volume 19 Issue 46 Sedar Supplement

SGML Handbook, Charles F. Goldfarb, 1990 Oxford University Press

Standards For The Preparation, Distribution and Citation of Canadian Judgments in Electronic Form, May 1996, Judges Computer Advisory Committee of the Canadian Judicial Council

Survey of Legal Issues Relating to the Security of Electronic Information, Information Technology Security Strategy Legal Issues Working Group, June 1995, Treasury Board of Canada

Sustaining Dialog, Ministry of the Attorney General, quarterly newsletter for the Sustain court filing project

Who Owns Copyright in Law Reports? Gérard Snow, 64 C.P.R. (2d) 49

17. **Appendix C: Glossary**

Authentication: identifying legitimate persons and machines.

Byte: eight binary digits (bits, that is ones and zeroes); capable of representing 256 numbers or characters (between 0 and 255, represented as 00000000 to 11111111); a fundamental unit of information transmission or storage in a computer.

CGM: Computer graphics metafile, an image file format.

Cryptography: the science of securing messages.

Digital signature: computer process designed for the same purpose as a handwritten signature; an electronic means of associating a person with a document; the result of applying specific technological processes to authenticate a document.

DTD: Document Type Definition, a prescribed document structure, expressed in the language SGML (q.v.); all documents filed under ERF must be structured to conform to the prescribed DTD.

E-mail: electronic mail, sent as a stream of bytes (q.v.) from one computer to another, through the Internet (q.v.) or a private network; may refer to the system or individual messages.

ERF: Electronic Regulatory Filing, a joint project of the National Energy Board and the Ontario Energy Board, for conversion of paper processes to digital systems facilitating the creation, exchange, use and reuse of regulatory information.

HTML: Hypertext Markup Language, used to create Word Wide Web (or simply, web) pages on the Internet with links, called hyperlinks, to other web pages; HTML is one document type definition (DTD, q.v.) described by the metalanguage SGML (q.v.).

Internet: A network of computer networks using an agreed communication protocol called Transmission Control Protocol/Internet Protocol (TCP/IP) that facilitates common services such as electronic mail, web pages and file transfers.

JPEG: an image file format from the Joint Photographic Experts Group, also called JPG files, suitable for storing and transmitting photographs in a computer system.

MPEG: a digital video compression format from the Motion Pictures Experts Group used to store and transmit movies in a computer systems.

PDF: Portable Document Format, a proprietary document file format of Adobe Systems Incorporated.

SGML: Standard Generalized Markup Language, a metalanguage used to describe document types such as HTML and XML (q.v.); separates content and structure from formatting and appearance.

XML: Extensible Markup Language, a subset of SGML (q.v.); expected to be the next generation document standard for the World Wide Web (q.v).

World Wide Web: the interlinked documents stored on computers connected to the Internet (q.v.), also called the web, hence the expression web page referring to a single document; document addresses frequently begin with www, an abbreviation for World Wide Web, as in www.neb.gc.ca or www.oeb.gov.on.ca.

Projet de système de dépôt électronique

Un projet conjoint de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario

Questions et commentaires

Le 15 janvier 1999

Toutes les publications de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario sont protégées par la *Loi sur le droit d'auteur* du Canada. Il est interdit de reproduire la présente publication, en tout ou en partie, sans l'autorisation expresse de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario. Pour obtenir de plus amples renseignements, veuillez communiquer avec le secrétaire de l'Office ou de la Commission aux adresses suivantes :

Office national de l'énergie
444, Septième Avenue S.-O.
Calgary (Alberta) T2P OX8
(403) 292-4800
http://www.neb.gc.ca

Commission de l'énergie de l'Ontario
2300, rue Yonge
C.P. 2319
Toronto (Ontario) M4P 1E4
(416) 481-1967
http://www.oeb.gov.on.ca

TABLE DES MATIÈRES

1. **Quel est l'objet du présent rapport?** 1

2. **Où en est le SDÉ?** 1

3. **Quelles questions ont été soulevées au sujet du SDÉ?** 1

4. **Quel est le fondement juridique du SDÉ?** 5

5. **Quels critères ont servi à la conception du SDÉ?** 7

6. **Quel niveau de protection le SDÉ pourra-t-il offrir?** 8

7. **Quels formats électroniques utilisera-t-on pour les documents du SDÉ?** 11

8. **Comment signera-t-on les documents dans le SDÉ?** 13

9. **Les documents du SDÉ seront-ils conformes aux règles de preuve?** 18

10. **Quelle sera l'incidence du SDÉ sur les renseignements confidentiels déposés auprès de l'Office et de la Commission?** 22

11. **Quelle sera l'incidence du SDÉ sur la justice naturelle et l'impartialité de la procédure?** ... 23

12. **Comment les documents seront-ils signifiés avec le SDÉ?** 25

13. **L'Office et la Commission ont-ils tenu compte de l'incidence du SDÉ sur la pratique du droit?** 26

14. **Cela signifie-t-il que l'Office et la Commission ont répondu à toutes les questions au sujet du SDÉ?** 27

15. **Annexe A : Autres organismes et gouvernements** 27

16. **Annexe B : Autres documents à consulter** 32

17. **Annexe C : Glossaire** 34

1. Quel est l'objet du présent rapport?

L'Office national de l'énergie (ONÉ) et la Commission de l'énergie de l'Ontario (CÉO) se préparent à convertir leurs systèmes d'information du papier à l'électronique. En vertu du Système de dépôt électronique (SDÉ) proposé, tous les participants aux processus de réglementation de l'Office et de la Commission transmettront et recevront l'information pertinente au moyen d'ordinateurs. Les documents papier feront alors exception.

Nota : Le présent rapport[1] a pour objet de fournir des renseignements généraux sur le SDÉ. Les propos qu'il contient sont d'ordre général et ne constituent pas un avis juridique. Les lecteurs qui recherchent un tel avis devraient consulter leurs propres conseillers.

2. Où en est le SDÉ?

À la suite d'une étude de faisabilité achevée en mars 1993, l'Office et la Commission ont procédé avec prudence, effectuant des études coûts-avantages et franchissant progressivement les étapes d'analyse, de conception et de mise en œuvre de projets pilotes. Durant ce temps, les entreprises de services publics réglementées, les intervenants et autres parties intéressées aux instances de l'Office et de la Commission ont participé à des ateliers et des séances de planification sur le SDÉ. Un prototype fonctionnel a déjà fait l'objet d'une démonstration. La mise en oeuvre initiale est prévue pour la fin de 1999.

3. Quelles questions ont été soulevées au sujet du SDÉ?

Deux catégories de questions ont été soulevées : celles qui découlent de la nouveauté relative du SDÉ (p. ex. «Comment puis-je signer un document électronique?») et celles qui prévoient des changements fondamentaux dans la façon dont l'Office et la Commission fonctionnent (p. ex. «Le SDÉ mènera-t-il à un plus grand nombre d'audiences par voie de mémoires?»).

Les questions de nouveauté se résoudront par le biais de la formation et de la connaissance du système. Toute nouvelle technologie soulève inévitablement des préoccupations au sujet des risques. Lors de l'arrivée des photocopieurs, par exemple, les gens ont manifesté certaines inquiétudes au sujet de la précision de la reproduction. Quand les télécopieurs sont apparus, on en a scruté l'utilisation. Les préoccupations

---

[1] Robin Nunn a rédigé le présent rapport pour le compte de la Commision de l'énergie de l'Ontario et de l'Office national de l'énergie (il remercie particulièrement Stephen McCann, Charles Mathis et Claire McKinnon pour leur aide).

portaient sur la précision des télécopies, les coûts inhérents aux envois par télécopieur et la légalité des documents télécopiés. Dorénavant, ces deux technologies, soit la photocopie et la télécopie, sont courantes, bien connues et utilisées presque sans réserve, à l'instar d'autres technologies familières comme le téléphone et la télévision. Bien qu'il existe toujours des problèmes, la plupart des premières préoccupations ont été résolues non pas en modifiant considérablement la technologie, mais en la comprenant mieux et en perfectionnant les procédés connexes.

Tout comme des inquiétudes se manifestent toujours au sujet des risques potentiels d'une nouvelle technologie, les gens ont aussi tendance à supposer le contraire, c'est-à-dire que les nouvelles machines, les ordinateurs en particulier, sont infaillibles. Ils semblent croire que, si les ordinateurs ne sont pas parfaits, ils sont alors inutiles. Songez à la question suivante : «Quels sont les risques de perdre un document parmi des milliers d'autres dans un système informatique?». On se pose rarement cette question dans le cas du système actuel de documents papier. Tout le monde sait qu'il est possible de perdre du papier. Aucun système informatique ou papier fonctionnel n'est à l'abri des risques. Les systèmes que l'Office et la Commission utilisent actuellement (papier ou électronique) ne sont pas parfaits. Un document papier peut être classé au mauvais endroit ou envoyé à la mauvaise adresse. Les mêmes erreurs peuvent se produire dans un système informatique. Grâce à une conception adéquate toutefois, il est possible de repérer et de corriger les erreurs, qu'il s'agisse d'un système électronique ou non. Il faut cependant comparer les risques inhérents au système proposé avec ceux du système actuel et non considérer la question comme un idéal impossible à atteindre.

Entre les préoccupations relatives aux risques, d'une part, et les attentes de perfection, d'autre part, une question se pose : n'y a-t-il pas danger de reproduire le système actuel sous forme électronique? Il pourrait être possible par ailleurs, après examen des motifs qui sous-tendent les procédures actuelles, d'adapter uniquement les aspects nécessaires au SDÉ. Par exemple, on utilise maintenant des signatures manuscrites et des affidavits sur les documents déposés auprès de l'Office et de la Commission. Naturellement, on a tendance à chercher une analogie électronique, comme la reproduction numérique d'une signature manuscrite. Est-ce nécessaire? Comment une image, que quiconque peut reproduire, se compare-t-elle à une signature manuscrite que seule la main du rédacteur peut réaliser? La signature manuscrite est-t-elle l'unique moyen de s'assurer de la légalité d'un document? Examine-t-on les signatures et est-ce qu'on s'attend à ce qu'il y ait contrefaçon? Ces questions démontrent qu'il faut éviter de reproduire le système actuel et en concevoir un meilleur. Pour obtenir de plus amples détails au sujet de ces questions particulières, consultez la section du présent rapport décrivant la façon dont on signera les documents dans le SDÉ.

Les ordinateurs sont impersonnels. Aucun humain n'assure la protection de l'information dans un ordinateur. Un mot de passe ou autre dispositif technique joue alors ce rôle. En conséquence, on a tendance à remettre en question la façon dont la machine impersonnelle effectuera toutes les choses qu'une personne fait pour assurer l'honnêteté du système. On s'attend également à ce que les ordinateurs fassent honneur à leur réputation de rapidité et d'efficacité surhumaines. Par conséquent, le temps

devient un problème là où il ne l'est peut-être pas maintenant. Par exemple, les utilisateurs demandent s'il est possible d'accéder au système informatique 24 heures sur 24 tous les jours. Nous ne nous posons pas cette question au sujet des systèmes manuels existants qui ne sont disponibles que durant les heures normales de bureau. On s'attend à ce que les ordinateurs fournissent des enregistrements vérifiés et qu'ils confirment chaque étape. Dans le système de documents papier actuel, cependant, nous acceptons souvent les risques du courrier ordinaire au lieu d'utiliser le courrier recommandé. Les ordinateurs traitent également des quantités énormes d'informations, qui sont pourtant intangibles et invisibles jusqu'à leur affichage à l'écran ou leur impression sur papier. Nous faisons implicitement confiance au texte composé et relié d'un livre, car la contrefaçon exigerait de l'habilité et des frais, alors que tout le monde peut faire apparaître des mots sur un écran ou un imprimé. Qui peut affirmer qu'ils sont authentiques? C'est pourquoi on pose au sujet des ordinateurs des questions que l'on ne poserait pas si les processus étaient plus humains et tangibles, moins techniques et complexes.

Peu importe les raisons de ces préoccupations et le type de système qui sera un jour mis en oeuvre, tous les intéressés doivent avoir confiance en lui. On peut exprimer des réserves d'ordre juridique simplement pour déterminer s'il faut faire confiance au nouveau SDÉ. En fait, la confiance est l'un des thèmes sous-jacents du présent rapport (voir, par exemple, la section traitant des tierces personnes de confiance et de l'infrastructure des systèmes à clés publiques). Le papier inspire confiance. Les documents papier servent à établir la vérité. La technologie informatique est nouvelle et n'inspire pas autant la confiance; elle suscite donc un réexamen des notions de confiance et de vérité.

Comme nous l'avons indiqué précédemment, les gens ont tendance à avoir des attentes irréalistes en ce qui a trait aux ordinateurs. Certaines personnes peuvent s'imaginer des audiences durant lesquelles les participants communiquent uniquement en tapant sur des claviers dans un centre de réglementation futuriste où le papier est proscrit. Le SDÉ est plutôt conçu pour améliorer les processus de réglementation de façons particulières axées non pas sur la technologie, mais sur des documents structurés et normalisés.

- Les principales améliorations reposent sur le dépôt central des documents électroniques. Au moyen d'un format international appelé langage standard généralisé de balisage (LSGB), toutes les informations du dépôt central posséderont une structure formelle. Cette structure, nécessaire pour stocker les documents (comprise dans la définition du type de document), permettra un échange et une gestion efficaces de ceux-ci. On prévoit que les informations seront plus complètes et plus faciles à trouver et à utiliser.

- Comme les informations se trouvent dans un dépôt central, les participants peuvent choisir celles qui les intéressent. On prévoit ainsi épargner les coûts de distribution de toute l'information à tous les participants tout en fournissant l'information demandée plus efficacement. On peut extraire des documents du système au lieu d'avoir à les envoyer à chacun.

- S'appuyant sur le système de base, les systèmes informatisés de gestion de l'information peuvent faciliter la tenue des réunions et des audiences. C'est ce qu'on appelle la salle d'audience automatisée. Dans sa forme la plus simple, elle permettra à chaque personne présente dans la salle de chercher et de récupérer des documents par voie électronique. Il ne faut pas confondre cela avec la transcription assistée par ordinateur qui permet de reproduire mot à mot le contenu des audiences. Ces transcriptions ne représenteront qu'un type de document stocké dans le dépôt central du SDÉ. Une autre technologie permettra la participation à distance. Parmi les autres possibilités, notons l'utilisation de logiciels permettant à des groupes de travailler ensemble à des moments et des endroits différents. Ce dernier concept s'appelle la salle d'audience électronique.

- Une autre amélioration proposée consiste à utiliser des outils de gestion de cas et d'ordonnancement du travail pour traiter les documents et améliorer l'établissement du calendrier.

- Les concepteurs du SDÉ proposent également de fournir une aide complète, non seulement sur l'utilisation du système informatique, mais également sur l'essence même du processus de réglementation.

Il importe de ne pas confondre le SDÉ avec d'autres innovations technologiques. Il ne s'agit pas d'un système de transcription assistée par ordinateur permettant d'obtenir des comptes-rendus exhaustifs instantanément. Il ne s'agit pas d'un système d'échange électronique de documents comme ceux qu'on utilise pour les transactions commerciales d'achat et de vente automatisées au moyen de bons de commande et de factures standard. Le SDÉ n'est pas un système d'imagerie qui stocke des images de documents. Ces techniques ainsi que d'autres peuvent faire partie du système proposé, mais elles ne sont pas essentielles. Les principaux avantages du SDÉ devraient se situer sur le plan de la création et du traitement des documents courants. Il est possible d'automatiser les documents électroniques et il n'est pas nécessaire de les imprimer, de les reproduire, de les relier ni de les livrer.

Il est également important de distinguer le dépôt central de documents du SDÉ d'un système d'enregistrement. Un bureau d'enregistrement, par exemple, sert à enregistrer des documents officiels. Ceux-ci sont refusés s'ils ne sont pas présentés dans la forme prescrite et seuls certains types de documents sont acceptés. L'information déposée auprès d'un bureau d'enregistrement a une incidence directe sur les garanties juridiques. Comparons le modèle du bureau d'enregistrement avec le système proposé de documents informatisés du SDÉ servant principalement à échanger de l'information. De nombreux types de documents sont acceptés afin que les participants puissent présenter leurs arguments. La plupart des documents déposés auprès de l'Office et de la Commission n'ont pas d'incidence directe sur les garanties juridiques. En réalité, bon nombre d'entre eux sont déposés avant le début d'une audience et n'ont aucune valeur juridique avant d'être considérés comme preuves admissibles. Même ceux qui sont acceptés en preuve n'ont habituellement pas la portée des documents d'enregistrement qui ont des conséquences juridiques directes. Ces différences ont une importance

considérable dans la conception du SDÉ proposé (consultez également la section traitant des autres systèmes électroniques).

Conclusion : le SDÉ constitue un moyen d'améliorer la communication et non une modification de l'essence même du processus de réglementation.

4. Quel est le fondement juridique du SDÉ?

Lorsqu'on a utilisé des documents électroniques pour la première fois dans le cadre de procédures judiciaires, on s'est interrogé au sujet de leur valeur par rapport aux documents papier. Dans certains cas, les lois ont résolu ces questions. Par exemple, de nombreuses lois confèrent maintenant la même valeur aux fichiers informatiques et aux documents papier (*Loi sur l'accès à l'information*, L.R.C. (1985), ch. A-1, par. 4(3), *Loi sur les sociétés par actions*, L.R.C. (1985), ch. C-44, par. 22(1), *Loi sur la preuve au Canada*, L.R.C. ch. C-5, par. 30(12), *Loi sur les brevets*, L.R.C. (1985), ch. P-4, al. 8(1)*l*), *Loi sur les sociétés par actions*, L.R.O. (1990), ch. B.16, par. 139(1), *Loi sur l'enregistrement électronique*, L.R.O. 1991 ch. E.44, *Loi sur l'enregistrement des droits immobiliers*, L.R.O. (1990), ch. L.5, par. 166(1), *Loi sur l'enregistrement des actes*, L.R.O. (1990), ch. R.20, par. 16(1) — consultez également la législation dans un nombre croissant d'États américains qui ont suivi l'exemple de l'Utah relativement à l'adoption de lois qui stipulent que, dans la correspondance avec le gouvernement, une signature numérique équivaut à une signature manuscrite).

À l'échelon fédéral, le rapport du Comité directeur de la stratégie - sécurité de la technologie de l'information, remis au Conseil du renouveau administratif en juin 1995, formulait les recommandations suivantes :

> «Bien qu'aucun obstacle juridique n'empêche le gouvernement fédéral d'utiliser la technologie de l'information, de mettre en oeuvre une stratégie sur la sécurité de la technologie de l'information ou de mettre en place un système à clés publiques pour le chiffrement des signatures numériques et des documents confidentiels, le Comité directeur recommande *que la loi soit révisée et éventuellement modifiée dans les domaines suivants :*
>
> - La *Loi d'interprétation* et la *Loi sur la preuve au Canada* devraient faire l'objet d'une révision pour clarifier les exigences en matière de preuves relatives aux fichiers électroniques, en ce qui a trait notamment aux conditions prescrites concernant les documents originaux écrits, les copies certifiées ou notariées, etc.
>
> - Les ministères devraient revoir leur propre mandat et les lois applicables pour s'assurer que la législation comporte des dispositions relatives à l'utilisation de ces nouvelles technologies de l'information.
>
> - La *Loi sur l'accès à l'information* et la *Loi sur la protection de la vie privée* devraient faire l'objet d'une clarification en ce qui a trait aux exigences relatives à la technologie de l'information et notamment :
>
> - les recherches et la surveillance par ordinateur;
> - les cartes à mémoire;
> - les pistes de vérification;

- la base de données centrale et les bases de données dont le contenu change fréquemment;
- les formalités relatives aux échanges d'information entre les institutions gouvernementales.

- Il faudrait adopter des lois concernant les systèmes à clés publiques pour définir les rôles et responsabilités des nombreuses parties en cause et restreindre la responsabilité financière du gouvernement fédéral. Il est important de nommer rapidement un ministre compétent relativement à l'application de telles lois.

- Il faudrait consulter le public au sujet des questions suivantes : l'utilisation de renseignements personnels sur les cartes à puce du gouvernement par exemple, l'échange de renseignements personnels entre les ministères ou entre les gouvernements fédéral et provinciaux et l'accès des forces de l'ordre aux renseignements chiffrés.

- Il faudrait clarifier les responsabilités juridiques des exploitants de babillards électroniques et des personnes qui diffusent de l'information sur des réseaux électroniques publics.

- Il faut réviser et probablement modifier les définitions des termes utilisés dans un contexte de communication électronique (p. ex., «communications privées», «place publique», «publication», «possession», «collection» et «divulgation»).

Un projet de loi fédéral, soit la Loi sur la protection des renseignements personnels et les documents électroniques (projet de loi C-54), traite de certaines de ces questions. La deuxième partie de ce projet de loi prévoit des solutions de rechange sur le plan électronique aux documents papier régis par les lois fédérales. Au lieu de modifier chaque loi fédérale séparément, le projet de loi modifierait l'ensemble de la législation. Les organismes gouvernementaux fédéraux seront autorisés à utiliser des moyens électroniques au lieu du papier, y compris les paiements, les formulaires et les dépôts électroniques.

L'ONÉ a présentement le pouvoir d'adopter des règles régissant la conduite de ses affaires (*Loi sur l'Office national de l'énergie*, L.R.C. (1985), ch. N-7, art. 8). Les *Règles de pratique et de procédure de l'Office national de l'énergie (1995)* (DORS/95-208), font explicitement référence au dépôt de documents. L'article 9 autorise tous les types de dépôts que l'ONÉ peut recevoir. Le même règlement rend toutefois obligatoire le dépôt de documents papier en plus des documents électroniques. Les règles font présentement l'objet d'une révision pour tenir compte des dépôts électroniques. La Commission de l'énergie de l'Ontario a également autorité sur le déroulement de ses audiences (*Loi sur l'exercice des compétences légales*, L.R.O. (1990), ch. S.22, art. 25.1) et les renseignements qui lui sont transmis (*Loi sur la Commission de l'énergie de l'Ontario*, 1998, art. 13). Ses règles font également l'objet d'une révision afin qu'elles accordent la même valeur aux dépôts de documents papier et de documents électroniques.

En l'absence de dispositions législatives plus précises sur le dépôt électronique, les principes de droits généraux établis en fonction des documents papier doivent être interprétés de nouveau dans un contexte électronique.

5. Quels critères ont servi à la conception du SDÉ?

Dès les premières étapes de planification, on a élaboré un ensemble de principes et de critères concernant le SDÉ, notamment :

- les systèmes et les processus employés dans le cadre de cette initiative doivent être efficaces, fiables et sûrs;
- les documents électroniques doivent satisfaire aux critères suivants :

  les documents électroniques doivent pouvoir durer et on doit être en mesure de conserver l'information documentaire (y compris la preuve) pendant la durée nécessaire à un tribunal d'archives;

  le chargement des documents dans le système doit être précis;

  le chargement des documents dans le système (c'est-à-dire le dépôt central des documents) doit se faire en temps opportun et nécessiter un minimum de manipulation;

  la présentation d'un document (c'est-à-dire les polices et la mise en page du document) déterminée par l'auteur doit, dans la mesure du possible, être conservée;

  les documents doivent être accessibles universellement, autrement dit, ils doivent être généralement récupérables et réutilisables peu importe le système ou le logiciel dont se sert l'utilisateur et qui est compatible avec les normes de systèmes ouverts;

  l'échange de documents doit être possible au moyen d'un éventail de véhicules de communication (p. ex., courrier électronique, disquettes, Internet, transfert de fichiers, CD-ROM);

- dans la mesure du possible, l'initiative s'appuiera sur une politique et des normes de systèmes ouverts non brevetés;
- les systèmes mis en oeuvre doivent être commandés par les utilisateurs et doivent satisfaire et équilibrer les besoins de tous les participants et du grand public;
- les systèmes et les processus mis en place doivent permettre de réduire à long terme les coûts de la réglementation et les délais de traitement;
- aux endroits où des services intérimaires sont offerts, ils doivent être rentables en soi et contribuer à la réalisation de l'objectif à long terme du SDÉ.

6. Quel niveau de protection le SDÉ pourra-t-il offrir?

Tous les systèmes informatiques nécessitent des mesures de sécurité. Quel type de sécurité est nécessaire et dans quelle mesure? La réponse dépend de questions incidentes, notamment : qui a accès aux ordinateurs et aux réseaux de communication? Qui possède un accès électronique? Qu'est-ce qui amènerait une personne à enfreindre la sécurité? Quelles infractions à la sécurité peut-on détecter? Quelles sont les conséquences des infractions à la sécurité? Quels sont les coûts inhérents à la protection? Quel niveau de protection offre le système papier actuel en comparaison? Les précautions en matière de sécurité entravent-elles l'utilisation normale du système? Et beaucoup d'autres questions détaillées.

Dans tout système informatique, il faut régler les questions suivantes :

- autorisation : l'autorisation d'utiliser le système (ce qui comprend non seulement les personnes, mais également les ordinateurs, c'est-à-dire les autres systèmes informatiques qui peuvent également accéder au système);
- authenticité : il faut déterminer si les utilisateurs sont réellement ceux qu'ils prétendent être et si l'information qu'ils fournissent est ce qu'elle doit être;
- disponibilité : il faut déterminer si le système est disponible et accessible lorsqu'il le faut;
- vérification;
- confidentialité;
- intégrité de l'information dans le système;
- respect de la vie privée.

Comme nous l'avons noté plus tôt, aucun système n'est parfait. Les systèmes de documents papier actuels ne sont pas parfaitement sûrs. Toutefois, on a jugé qu'ils étaient acceptables. Même les classeurs verrouillés derrière des portes verrouillées peuvent ne pas résister à un intrus déterminé. Le feu et l'eau peuvent endommager les dossiers papier comme les fichiers électroniques. Le système informatique d'un organisme peut subir des dommages non seulement de la part d'un individu utilisant la technologie, comme le légendaire pirate informatique, mais également d'une personne en mesure de perturber le fonctionnement de tout système, comme un employé mécontent. Il y a toujours un risque, mais aucune garantie de sécurité absolue.

En utilisant des techniques de sécurité informatiques acceptables, le SDÉ proposé peut s'avérer plus sûr que le système actuel. Présentement :

- le document papier peut parvenir à la mauvaise adresse ou se perdre dans le courrier;

- le public peut manipuler les documents originaux auxquels il a accès et peut, par conséquent, les endommager, les modifier ou les perdre;

- les dossiers existants peuvent être incomplets;

- il peut être difficile de retrouver les dossiers anciens;

- les dossiers papier actuels peuvent comporter des erreurs;

- il n'y a pas de système de secours ou de sauvegarde analogue à celui d'un système électronique dont on peut se servir après un sinistre ou durant des interruptions courantes, comme le déménagement vers un nouvel emplacement;

- même les documents ayant un statut particulier, comme les affidavits signés, ne sont pas particulièrement sûrs de nos jours. Il serait inhabituel pour un tribunal de confirmer l'identité ou l'autorité de la personne qui a signé ou de comparer les signatures sur l'affidavit avec toute autre pièce d'identité, comme un permis de conduire ou un passeport.

Tout comme le papier pose des problèmes de sécurité particuliers (accès aux locaux, cadenas à combinaison, clés), les systèmes informatiques ont aussi les leurs (mots de passe, copies de sauvegarde, panne de courant). Un système informatique bien conçu offre autant sinon plus de sécurité qu'un système papier. Comme tous les documents se présentent sous forme électronique, il est possible d'en fournir des copies identiques au besoin. On peut contrôler et vérifier l'accès aux fichiers. Les techniques de vérification par ordinateur peuvent réduire les erreurs. La normalisation des formats peut améliorer la cueillette et la récupération des données. L'automatisation peut réduire les erreurs humaines.

Comme il est possible de rendre les systèmes informatiques plus sûrs que les systèmes papier, la sécurité informatique ne consiste pas uniquement à protéger le système, mais également à trouver un équilibre entre la sécurité et la facilité d'utilisation. Une sécurité trop importante peut s'avérer aussi inefficace qu'une sécurité insuffisante. Par exemple, on peut rendre un système informatique très sûr en attribuant un mot de passe unique à chaque document et en utilisant un programme particulier pour y accéder. Un intrus devrait connaître dix mots de passe et savoir comment utiliser dix programmes pour lire dix documents. Il est techniquement facile de créer une telle barrière. Malheureusement, les utilisateurs autorisés seraient également confrontés à ce même obstacle. Personne ne voudrait utiliser un tel système sûr, mais inefficace. En effet, les utilisateurs autorisés oublieraient probablement un bon nombre des mots de passe ou les noteraient sur une feuille et créeraient ainsi un nouveau problème de sécurité à l'égard de la protection de la liste des mots de passe.

Les documents papier sont si familiers que nous nous informons rarement des exigences en matière de sécurité. Quels éléments nous inspirent confiance à leur égard? Les mêmes s'appliquent aux documents numériques, notamment :

- l'authenticité de la personne — un document devrait indiquer qui l'a signé;

- l'authenticité du document — un document devrait indiquer ce que la personne a signé.

Prenons une lettre ordinaire signée par la personne qui l'a rédigée. De nombreux éléments pourraient servir à en prouver l'authenticité : un graphologue pourrait témoigner au sujet de la signature, un expert en matériaux pourrait analyser le papier et l'encre, alors que l'adresse, l'adresse de retour, le cachet de la poste, le timbre et le contenu pourraient tous contribuer à nous inspirer une confiance absolue en ce document. Chacun de ces éléments pourrait toutefois être contrefait. L'écriture peut tromper même un expert ou être tout simplement illisible. Les témoins peuvent mentir.

Dans un système informatique, les techniques d'authentification doivent être conçues de manière à prévenir la contrefaçon. Le système doit faire en sorte que la personne qui signe le document ne puisse nier l'avoir fait. Toute technique utilisée couramment devrait être efficace. À l'instar d'une signature manuscrite, cela devrait être facile à faire. On peut appliquer aux ordinateurs bon nombre des techniques employées dans les systèmes papier, y compris l'accusé de réception (comme dans le cas du courrier recommandé) et la vérification du trafic de messages (suivi et enregistrement du courrier).

Les documents électroniques sont-ils sûrs? Bien qu'aucune décision définitive n'ait été prise au sujet des programmes de sécurité particuliers à utiliser avec le SDÉ, la conception du système de documents électroniques proposé prévoit des logiciels servant à prévenir les modifications non autorisées des documents. Le système sera en mesure de détecter si l'information a été modifiée, à quel moment elle l'a été la dernière fois et par qui. À cet égard, les documents papier, qui sont faciles à modifier, sont moins sûrs que les documents électroniques du SDÉ proposé.

Les documents électroniques peuvent-ils être contrefaits? Dans le cas des instances réglementaires, la contrefaçon des documents est peu probable. Le secrétaire de l'Office ou de la Commission n'examine pas présentement la signature manuscrite de l'avocat ou du témoin qui dépose un document papier afin d'être certain qu'il s'agit d'une signature authentique. Un document électronique, par contre, peut comporter un code de sécurité (une signature numérique, dont on parlera ailleurs dans le présent rapport) servant de signature manuscrite.

Un système électronique doit également être en mesure de s'assurer que la personne qui envoie un document ne puisse nier l'avoir fait et qu'une personne recevant un document ne puisse nier l'avoir reçu. Le SDÉ proposé comporte là encore des éléments relatifs à la non-répudiation et à la vérification des transactions.

L'authentification d'un document est étroitement liée à la vérification du contenu. Les techniques de signature des documents devraient offrir un moyen de vérifier non seulement à quel document se rapporte la signature, mais aussi que le document signé est complet et authentique.

Dans certains systèmes informatiques, même les mesures de sécurité qui protègent le système sont confidentielles, et l'emplacement ou peut-être même l'existence des systèmes sont tenus secrets. Dans la région, par exemple, un grand immeuble de banlieue non identifié abrite les systèmes informatiques d'une importante société multinationale. L'immeuble ne porte pas de nom, seulement une adresse. Toute organisation, même pourvue d'une sécurité aussi serrée, doit être prête à divulguer au besoin les détails nécessaires au sujet de son système informatique pour prouver l'authenticité de fichiers informatiques en cour (consultez également la section traitant de la preuve informatique).

De nombreuses organisations ont recours aux mêmes techniques de sécurité informatique, y compris les banques et les forces de l'ordre, qui ont également besoin de systèmes sûrs.

7. Quels formats électroniques utilisera-t-on pour les documents du SDÉ?

De préférence aux formats exclusifs, le SDÉ utilise des formats ouverts internationaux lorsque cela est possible. En conséquence, le SDÉ n'accepte pas les formats propres à des produits comme Word de Microsoft ou WordPerfect de Corel. Comme la plupart des documents déposés contiennent du texte (c'est-à-dire des mots, des tableaux, des graphiques, etc.), l'architecture sous-jacente repose sur le langage standard généralisé de balisage (LSGB) international. On prévoit également que les formats XML et HTML serviront également à distribuer de l'information, bien que les documents acceptés au dépôt central doivent être en LSGB. On peut stocker certains documents contenant par exemple des données numériques volumineuses dans des formats courants de base de données relationnelles. Bien que les images de documents produites par lecture optique ou par télécopie directe puissent servir dans des cas exceptionnels, l'architecture du SDÉ repose sur des formats à base de caractères se prêtant à des recherches. (Consultez également le glossaire de l'annexe C pour obtenir de l'aide concernant les termes techniques utilisés dans la présente section).

Il n'existe pas de format de document parfait ni de moyen infaillible pour chercher de l'information dans un grand dépôt central. L'Office et la Commission ont choisi un format permettant de coder de l'information contextuelle dans le document même. Cette information supplémentaire, outre les mots, peut servir à chercher des documents, à les convertir d'un format à l'autre ou à effectuer d'autres traitements au moyen des informations additionnelles codées dans le document. Grâce au LSGB les documents peuvent être exploités comme des bases de données, au lieu d'être simplement stockés.

On peut procéder à des recherches mot à mot avec les autres formats, mais la recherche plein texte familière est susceptible de se buter à des problèmes de parasites et autres concepts connexes issus de la théorie fondamentale de l'information. En deux mots, lorsqu'on cherche dans un grand dépôt central, on obtient trop ou pas assez d'information, mais rarement l'information exacte nécessaire. Les transcriptions de témoignages, par exemple, compliquent la recherche mot à mot étant donné toutes les

subtilités du langage humain. Un témoin peut parler souvent de «il», par exemple, en le décrivant en détail, alors que seule une référence indirecte située bien avant dans le texte explique ce qu'est «il». Les mots clés qui apparaissent fréquemment dans une base de données sur l'énergie, comme «gaz naturel», ne sont pas plus utiles pour trouver des passages pertinents que des mots comme «il». On peut indexer de nombreux formats de document séparément pour améliorer la recherche, mais cet index n'est pas contenu dans le format même du document. L'indexage par mot clé présente aussi des inconvénients, surtout s'il est mécanique. Par contre, on peut indexer un document en LSGB pendant sa création, les éléments et les attributs voulus étant intégrés dans le document par l'auteur.

Les formats qui combinent la mise en forme et le contenu, comme ceux des logiciels de traitement de textes et Adobe Portable Document Format (PDF), sont conçus pour bien faire paraître le texte et les graphiques sur une page. Ils tentent de reproduire électroniquement le document papier. Cependant, la mise en forme en souffrira si le dispositif de sortie, habituellement l'imprimante ou l'écran, ne peut reproduire les caractères et d'autres caractéristiques utilisées par l'auteur du document. Ils produisent également des documents beaucoup plus volumineux que le LSGB et consomment plus de ressources en matière de communication et de stockage. La séparation de la forme et du contenu qu'offre le LSGB augmente les possibilités de réutilisation des documents; la conversion entre documents LSGB ou du LSGB à d'autres formats, comme le PDF, est beaucoup plus facile qu'à partir d'un format contenant moins d'informations intégrées.

Le LSGB est devenu une norme internationale arrivée à maturité, contrairement aux formats exclusifs qui changent fréquemment. L'Office et la Commission ont noté les problèmes éprouvés par d'autres tribunaux aux prises avec de prétendues mises à niveau. Par exemple, lorsqu'une nouvelle version du logiciel de traitement de texte approuvé arrive sur le marché, les règles des tribunaux et les systèmes informatiques de tous les participants peuvent nécessiter des modifications pour utiliser le nouveau format.

Le LSGB est complexe et cette complexité augmente les coûts d'analyse, de conception, de développement et de maintenance. Le coût initial d'un système LSGB peut être beaucoup plus élevé que celui d'un système reposant sur des formats exclusifs, en raison notamment de l'élaboration de la définition du type de document, et le LSGB peut nécessiter des outils logiciels supplémentaires pour en permettre l'utilisation. Toutefois, les documents LSGB sont indépendants du logiciel qui les a créés. Les outils peuvent être différents, mais les documents au coeur du système peuvent être consultés par tous les participants, que ce soit maintenant ou dans l'avenir, peu importe les outils brevetés dont ils se servent. De plus, la puissance des outils LSGB a augmenté rapidement alors que leur coût diminuait.

Bien qu'il soit simple et portable, le langage HTML n'est pas extensible et ne peut pas s'adapter à un contenu particulier. Par conséquent, comme nous l'avons indiqué précédemment, la capacité de recherche d'un document HTML particulier dans un grand dépôt central est limitée. Notons en outre que le langage HTML ne peut

accepter que les formulaires simples à remplir et les liens hypertextes unidirectionnels. Bien que chaque nouvelle version du langage HTML en augmente la capacité, les modifications logicielles permettant d'intégrer les nouvelles versions exigent du temps et des ressources. De toute façon, toutes les versions de ce langage combinent la mise en forme et le contenu dans une définition unique du type de document.

Contrairement au HTML, le XML offre un grand nombre des avantages du LSGB. Sans décrire en détail ces langages de balisage, il est préférable de choisir le XML plutôt que le HTML pour les raisons suivantes notamment : la séparation du contenu de la mise en forme, la possibilité d'utiliser des feuilles de style différentes, l'amélioration des liaisons, la liberté de définir les types de documents et l'utilisation croissante du XML dans l'industrie. Comme le XML est plus simple que le LSGB, le développement des logiciels sera également plus facile.

Malgré l'intérêt croissant que l'on porte au XML comme remplaçant du HTML, la capacité ultime de formaliser la structure des documents réside dans le LSGB. Comme il s'agit du métalangage sous-jacent à ces autres formats, l'utilisation du LSGB ouvre implicitement la porte à celle du HTML et du XML. La mise en oeuvre du LSGB par l'Office et la Commission sera compatible avec le XML. Parmi les autres formats ouverts pris en charge, mentionnons le JPEG, le MPEG et le CGM, qui permettent de stocker un éventail d'éléments graphiques et d'informations multimédias sans compromettre les exigences relatives à l'archivage. D'autres formats ouverts seront pris en charge au besoin.

8. **Comment signera-t-on les documents dans le SDÉ?**

Pendant des siècles, diverses lois ont exigé que les mots soient écrits, signés, certifiés, notariés ou même présentés dans une forme prescrite. Ces exigences ont permis de prévenir les différends sur le contenu exact de ce qui avait été dit. L'obligation de consigner par écrit n'équivaut cependant pas nécessairement à celle de signer. Un écrit peut ne pas être signé. Il permet de saisir les idées à de nombreuses fins, y compris l'utilisation à titre de preuve. Les signatures identifient et lient formellement une personne à l'écrit de façon que, en l'absence de contrefaçon, elle ne puisse renier l'écrit.

Les documents ayant une valeur juridique sont souvent signés à la main. Il semble naturel, par conséquent, d'exiger que le système informatique comporte une analogie électronique à la signature manuscrite. Avant d'aller de l'avant, toutefois, il faut d'abord noter qu'une signature manuscrite ne constitue pas l'unique moyen ou même le moyen le plus courant de conférer une valeur juridique à un document. Une signature représentant un nom écrit à la main n'est pas toujours nécessaire. Une marque comme un «X» servant de signature peut être acceptable. Un timbre ou un fac-similé peut être accepté, comme on le voit couramment sur les chèques et autres effets de commerce. Une signature créée mécaniquement peut être considérée en droit comme une signature humaine. Les tribunaux au Canada, au Royaume-Uni et aux États-Unis ont statué que les timbres mécaniques et autres signatures reproduites ont

force de loi. Même une signature illisible a été acceptée (consultez, par exemple, *R. v. Kapoor* (1989), 52 C.C.C. (3d) 41). En outre, le mandant n'est pas tenu de signer un document. Un mandataire peut le faire à sa place. Une procuration peut autoriser une personne à signer de nombreux documents. Au niveau gouvernemental, la loi peut accorder des pouvoirs de signature.

La loi a généralement fait preuve d'une souplesse suffisante pour s'adapter à la nouvelle technologie en acceptant les nouvelles formes d'écriture et de signature ou même en évitant tout simplement ce type d'exigence. Aux niveaux fédéral et provincial, l'interprétation des dispositions de la loi relatives à l'écriture tient compte depuis longtemps de divers médias, comme l'exprime l'extrait suivant :

> «écrit» Mots pouvant être lus, quel que soit leur mode de présentation ou de reproduction, notamment impression, dactylographie, peinture, gravure, lithographie ou photographie. La présente définition s'applique à tout terme de sens analogue. (*Loi d'interprétation*, L.R.C. (1985), ch. I-21, art. 2).

Comme nous l'avons indiqué ailleurs dans le présent rapport, une définition comme celle-ci peut s'avérer trop restrictive dans le cas de l'informatique, mais elle illustre la souplesse des concepts.

On a adopté des lois particulières pour éliminer les obligations relatives à l'écriture et à la signature. Le gouvernement fédéral et certaines provinces ont mis en application la Convention des Nations Unies sur les contrats de vente internationale de marchandises, qui stipule que les contrats de vente ne doivent pas obligatoirement être écrits. L'Ontario, par exemple, a éliminé cette exigence dans sa *Loi sur la vente d'objets* (L.R.O. (1990), ch. S.1; consultez également la *Loi sur la vente internationale de marchandises*, L.R.O. (1990), ch. I.10).
Dans un système informatique, comme dans un système papier, les signatures manuscrites ne constituent pas nécessairement l'unique moyen d'authentifier des documents. Selon les circonstances, il est possible de le faire au moyen d'un marquage électronique, comme l'information contenue dans une adresse électronique, d'un nom tapé dans le texte du message, d'un fac-similé de signature sous forme d'image numérique ou de processus nécessitant des mots de passe et des numéros d'identification personnelle. Dans certains systèmes de dépôt électronique, comme SEDAR (décrit ailleurs dans le présent rapport), le déposant doit conserver une feuille signée à la main à l'appui du dépôt électronique. Revenu Canada utilise une technique similaire pour les déclarations de revenus transmises par voie électronique. Le déposant, qui conserve la signature manuscrite du contribuable, agit à titre de représentant de Revenu Canada pour authentifier la déclaration.

Aux fins de l'examen de la question de la signature, on considère qu'aucune des formules mentionnées ci-dessus ne constitue une signature numérique, car il ne s'agit pas d'un concept visuel. La signature numérique résulte plutôt d'un calcul mathématique appliqué au document. Autrement dit, elle utilise un «code secret». Il n'est pas nécessaire que l'expéditeur soit mathématicien; il a simplement besoin d'un logiciel qui effectue le calcul approprié et joint la signature au document. Celle-ci ne

modifie pas le contenu du document, mais s'y ajoute. Dans certains systèmes, le code peut servir à brouiller (chiffrer) le document entier afin de le rendre confidentiel, mais le chiffrement des documents ne fait pas nécessairement partie d'un système de signatures numériques. Que le message soit chiffré ou non, une signature numérique peut néanmoins servir à déterminer si des modifications non autorisées ont été apportées au texte du message.

Le concept de signature numérique est probablement déroutant et certainement nouveau pour la plupart des gens. C'est pour cette raison qu'on en traite dans une section distincte, bien qu'il soit étroitement lié à d'autres questions, comme la sécurité des systèmes et l'admissibilité de la preuve.

Pour être efficace, le code de signature est calculé de manière qu'il identifie le signataire, que personne ne puisse le créer outre le signataire et que le destinataire du document puisse le vérifier. Il convient de noter que le logiciel du destinataire n'a pas besoin du code secret de l'expéditeur, appelé clé privée, mais seulement de la clé publique correspondante servant à vérifier la signature.

Un logiciel de signature numérique a habituellement recours à des concepts mathématiques complexes, comme les propriétés des nombres premiers, les fonctions de condensation et le chiffrement asymétrique, qui dépassent le cadre de la présente analyse. Du point de vue des utilisateurs, la signature numérique peut se résumer à l'ajout d'une chaîne de caractères inintelligibles au bas d'un message électronique. Le logiciel du destinataire traite cette chaîne de caractères pour authentifier la signature et le message. La caractéristique fondamentale d'une signature numérique, c'est qu'il est possible de l'associer à la personne qui l'a créée. Seul le détenteur de la clé privée peut produire la signature. Il n'est pas nécessairement possible d'associer à leur auteur les formes de signatures non mathématiques indiquées plus haut, comme un nom dactylographié ou un fac-similé numérique, car quiconque peut les reproduire.

Les motifs fondamentaux de l'utilisation des signatures sont plus importants que le simple aspect mécanique. Une signature sert à attester l'authenticité d'un document. Elle prouve que le signataire a approuvé le contenu du document et qu'il en accepte les conséquences. Le signataire ne peut répudier une signature valide. Tout système (papier ou électronique) doit indiquer de façon efficace qui a signé (authentification du signataire) et ce qui a été signé exactement (authentification du document) afin que les frais inhérents à l'utilisation des signatures soient minimes.

En règle générale, dans les instances de réglementation, le destinataire d'un document ne vérifie pas la signature qui y apparaît, bien qu'il puisse le faire en cas de besoin. C'est plutôt le processus au moyen duquel le document est créé et remis au destinataire qui lui confère sa valeur. Une preuve déposée au préalable, comme une prévision économique par exemple, doit être authentifiée durant l'audience. La signature qui y est apposée a peu de valeur tant qu'un témoin n'a pas attesté le document et eu l'occasion de l'expliquer, de le corriger ou de le mettre à jour.

Des procédures appropriés peuvent remplacer une signature manuscrite. En voici des exemples courants :

- la banque électronique à domicile,
- le paiement par carte de crédit au téléphone,
- l'enregistrement de valeurs mobilières en ligne,
- l'achat de valeurs mobilières auprès d'un courtier.

Chacun de ces exemples utilise différents systèmes de protection pour s'assurer qu'une personne ou son mandataire est lié par l'opération, malgré l'absence de signature manuscrite.

Comme il n'y a présentement aucune méthode formelle à l'Office et à la Commission permettant de détecter la fraude ou la contrefaçon de documents signés, le système informatique proposé ne peut augmenter de façon importante les risques à cet égard. Le système permet plutôt d'automatiser le processus de vérification des signatures. Une disposition générale relative au préjudice peut exempter un participant des exigences du système selon les circonstances.

Pour les signatures numériques, il est nécessaire d'utiliser un système à clés publiques avec des tierces personnes de confiance ou des autorités certificatrices. On peut associer une signature manuscrite à une personne en la regardant signer et en comparant des échantillons d'écriture. Une signature numérique est simplement une chaîne de chiffres. On peut l'associer à quelqu'un en demandant à un tiers de conserver des registres permettant de vérifier si la chaîne de chiffres a été attribuée à la personne qui prétend posséder la signature numérique en question. Autrement dit, un tiers peut être responsable de l'émission et de la révocation des signatures numériques et surveiller de façon générale le système.

Le projet de loi C-54 du gouvernement fédéral (traité ailleurs dans le présent rapport) prévoit des règles qui considèrent certaines technologies comme étant acceptables pour les signatures électroniques sécurisées. Certaines des questions dont on doit tenir compte dans l'élaboration de ces règles sont exprimées en ces termes :

> «Le gouverneur en conseil ne peut prévoir une technologie ou un procédé que s'il est convaincu qu'il peut être établi ce qui suit :
> a) la signature électronique résultant de l'utilisation de la technologie ou du procédé est propre à l'utilisateur;
> b) l'utilisation de la technologie ou du procédé pour l'incorporation, l'adjonction ou l'association de la signature électronique de l'utilisateur au document électronique se fait sous la seule responsabilité de ce dernier;
> c) la technologie ou le procédé permet d'identifier l'utilisateur;

d) la signature électronique peut être liée au document électronique de façon à permettre de vérifier si le document a été modifié depuis que la signature électronique a été incorporée, jointe ou associée au document.» (par. 48(2)).

Le projet de loi établit également un lien entre le concept de signature électronique sécurisée et la loi de la preuve en ces termes (consultez également la section traitant de l'authentification) :

«Le gouverneur en conseil peut prendre des règlements établissant des présomptions relativement aux documents électroniques portant une signature électronique sécurisée, y compris des règlements visant :
a) l'association de signatures électroniques sécurisées à des personnes;
b) l'intégrité de l'information contenue dans un document électronique portant une signature électronique sécurisée;
c) la manière de prouver toute question visée aux alinéas a) ou b).»(art. 31.4).

Le projet de loi C-54 fait une distinction entre les signatures sécurisées en général et la technologie particulière des signatures numériques. Il se peut aussi que l'on établisse ultérieurement par règlement d'autres technologies de signature sécurisée, comme la transmission de données biologiques. Le projet de loi définit la «signature électronique» et la «signature électronique sécurisée», cette dernière exigeant l'emploi de la technologie prescrite. Une signature électronique sécurisée satisferait également aux exigences de la loi relatives aux sceaux.

La loi proposée ferait en sorte que les documents électroniques satisfassent aux exigences des lois énumérées en annexe. Si la loi exige un document original, la version électronique nécessiterait une signature électronique sécurisée. Les déclarations faites sous serment, comme les affidavits, pourraient l'être de façon électronique au moyen de deux signatures électroniques sécurisées, soit celle de la personne qui fait la déclaration et celle de la personne autorisée à l'assermenter. De même, les documents qui doivent être signés par un témoin pourraient comporter deux signatures électroniques sécurisées, soit celle du signataire et celle du témoin.

Si les signatures sécurisées sont plus sûres que les signatures écrites, nous avons maintenant de nouvelles catégories de confiance. Dans un monde de documents papier, nous utilisons couramment la signature et occasionnellement la protection supplémentaire d'un témoin. En vertu de certaines lois, n'importe qui peut servir de témoin. D'autres lois exigent un témoin officiel, comme un commissaire à l'assermentation ou un notaire. La signature électronique sécurisée fait intervenir un nouveau type de témoin, soit l'autorité certificatrice. Certaines situations pourraient toujours exiger l'équivalent électronique d'un affidavit, mais, dans bon nombre de cas, une seule signature sécurisée pourrait suffire. Par exemple, la présence d'un témoin impartial peut s'avérer nécessaire pour confirmer l'état mental du signataire. Cependant, lorsque le témoin impartial ne fait que confirmer la signature du document sans vérifier les intentions du signataire, seule une signature sécurisée pourrait être nécessaire. En d'autres mots, l'idée de la signature numérique d'un témoin soulève la question suivante : de quoi la seconde signature témoigne-telle?

Les systèmes qui traitent les signatures électroniques sont complexes. L'une des façons les plus efficaces de passer du papier aux documents électroniques consiste alors à éliminer toute signature inutile. Les règles de l'Office et de la Commission devraient peut-être faire l'objet d'un examen pour s'assurer que les signatures ne sont pas exigées simplement parce qu'elles l'ont toujours été. Par exemple, la signature sous serment des affidavits et des documents notariés peut constituer un moyen de relier des sanctions pénales au dépôt de faux. Le même objectif peut être atteint au moyen d'une règle ou d'un règlement général autorisant l'utilisation de systèmes informatiques pour produire des signatures, accompagné de sanctions pour le dépôt de faux, sans exiger des serments distincts pour chaque document (consultez, par exemple, les Règles de l'assurance-emploi DORS/96-332, art. 90, 91).

9. Les documents du SDÉ seront-ils conformes aux règles de preuve?

La preuve sur laquelle la décision d'un tribunal se fonde doit être pertinente et fiable. Si elle n'est pas pertinente, elle ne peut pas aider le décideur. Si elle n'est pas fiable ou s'il n'existe aucun moyen d'en déterminer la fiabilité, elle ne peut pas servir à établir les faits entourant la cause. Toute preuve inappropriée ou douteuse est tout simplement rejetée ou admise sans toutefois être prise en compte dans la décision. Dans le cas du SDÉ proposé, la question consiste alors à déterminer s'il fournira des preuves pertinentes, fiables et admissibles.

Parmi les diverses catégories de preuves utilisées pour démontrer le bien-fondé d'une cause, comme le témoignage oral, la preuve écrite, la preuve matérielle, etc., c'est la preuve documentaire qui s'avère la plus pertinente à l'égard du SDÉ proposé. Avant qu'un document puisse être admis en preuve et versé au dossier, il doit passer plusieurs épreuves. Par exemple, il faut l'authentifier, c'est-à-dire démontrer qu'il est authentique. La soi-disant règle de la meilleure preuve nécessite également le document original s'il est disponible. Ces règles de preuve, entre autres, comportent de nombreuses exceptions. Les documents très anciens, par exemple, sont généralement considérés comme étant authentiques.

Les documents informatiques sont admissibles en cour à titre de preuves documentaires en vertu des principes de la *common law*. En outre, il existe une disposition législative spécifique pour les documents, y compris les documents informatiques, créés dans «de cours ordinaire des affaires» (*Loi sur la preuve au Canada*, L.R.C. ch. C-5, art. 30, *Loi sur la preuve*, L.R.O. (1990), ch. E.23, art. 35).

Les termes employés dans la *Loi sur la preuve au Canada* ne précisent pas la façon de s'assurer de l'admissibilité des documents informatiques. Même s'ils sont admissibles, il n'existe aucune norme particulière permettant de s'assurer que le tribunal y accordera l'importance voulue dans ses délibérations. Les tribunaux examineront l'ensemble des circonstances relatives à la création des documents. En règle générale, l'admissibilité et l'importance des documents informatiques dépendent de la fiabilité des processus de saisie, de mise en mémoire et de récupération de l'information :

> «La nature et la qualité de la preuve présentée au tribunal doivent refléter les faits entourant l'ensemble du processus de tenue des dossiers et, dans le cas des documents informatiques, des méthodes et procédés relatifs à la saisie des données, à la mise en mémoire ou à l'information ainsi qu'à sa récupération et à sa présentation» (*R. c. McMullen* (1979) 47 CCC (2d) 499 à 506, 25 OR (2d) 301, 100 DLR (3d) 671).

Autrement dit, il n'existe aucun moyen de *garantir* qu'un document informatique particulier sera admissible et qu'on y accordera l'importance voulue. Évidemment, un tribunal de réglementation n'est pas une cour de justice soumise à toutes les nuances de la loi sur la preuve.

De toute façon, l'enquête dans un différend sur la validité des documents du SDÉ ne porterait pas essentiellement sur une feuille de papier ou un document informatique donné. Elle porterait sur le système de tenue de dossiers qui a produit le document. C'est donc dire que le SDÉ, soit l'ensemble du processus de tenue de dossiers dont il est question ci-dessus, doit être fiable et satisfaire aux normes de l'industrie.

Bien que les lois fédérale et provinciales sur la preuve fassent référence aux documents informatiques, elles ne font pas de distinctions subtiles, comme la différence entre l'imagerie et la reconnaissance optique des caractères. Le systèmes d'imagerie copient les documents sans séparer les parties distinctes de l'image en lettres et en chiffres. L'imagerie peut comporter des erreurs qui se produisent durant la saisie de l'image et à cause de la capacité limitée des systèmes numériques. C'est-à-dire que les images du monde réel peuvent contenir plus d'information qu'il n'est possible d'en saisir dans un espace de stockage raisonnable dans le monde numérique. Contrairement à l'imagerie, la reconnaissance optique des caractères tente de séparer les parties significatives de l'image, mais elle prête à interprétation, comme par exemple, est-ce qu'un point est un signe de ponctuation ou simplement une tache sur l'image? On crée encore une autre forme de document informatique en copiant un fichier d'un disque à un autre. À moins de vérifier la copie octet par octet, on ne peut pas supposer qu'elle soit exacte, même si elle l'est habituellement. Ces différentes façons de créer de tels documents sont regroupées sous la rubrique documents informatiques. Cependant, leur fiabilité varie. Il est possible de vérifier l'exactitude du dernier type de copie, mais peu d'utilisateurs de la reconnaissance optique des caractères pourraient s'attendre à un texte parfait chaque fois. L'imagerie se situe quelque part au milieu de l'échelle de la fiabilité selon la qualité des documents papier originaux, le perfectionnement du matériel d'imagerie, les algorithmes d'imagerie utilisés (p. ex., sans perte ou compression avec perte) ainsi que la taille et le format des images stockées. (À cet égard, il convient de remarquer que Revenu Canada a publié une circulaire d'information dans le but d'inclure l'imagerie comme méthode de conservation des dossiers fiscaux. Consultez la Circulaire d'information 78-10R2SR du 10 février 1995, qui exige que les dossiers soient conservés conformément aux normes établies dans le document intitulé «Microfilms et images électroniques - preuve documentaire» (CAN/ONGC - 72.11-93) de l'Office des normes générales du Canada.

En ce qui a trait aux copies, il n'y a aucun moyen d'être certain de ce qu'un tribunal dirait au sujet de la destruction d'originaux utilisés pour créer des documents informatiques. Si la destruction fait partie du cours ordinaire des affaires, les

documents pourraient alors réussir cette épreuve. Dans le cas contraire, elle pourrait être considérée comme une entrave et une supercherie (consultez également la section traitant des questions d'exercice professionnel). La *Loi sur la preuve* comporte des dispositions particulières concernant la destruction de documents signés que l'on a photographiés (c'est-à-dire microfilmés), mais n'inclut pas de façon précise les documents numériques (*Loi sur la preuve au Canada*, L.R.C. (1985), ch. C-5, art. 31, *Loi sur la preuve*, L.R.O. (1990), ch. E.23, art. 34).

D'autres principes pourraient s'appliquer en matière de preuve outre le cours ordinaire des affaires mentionné ci-dessus. La nécessité de soumettre des faits exacts au tribunal sous-tend tout le droit de la preuve. Pour satisfaire à cette exigence, les tribunaux préfèrent :

- des documents réalisés à la même époque que les événements qu'ils décrivent (car la mémoire humaine oublie);
- des documents fondés sur la connaissance personnelle (et non sur des ouï-dire potentiellement douteux);
- des faits et non des opinions (la phrase familière «seulement les faits, s. v. p.», laissant les opinions aux experts et au tribunal);
- des documents originaux plutôt que des copies (principe qui a vu le jour dans un monde de documents papier où les copies ne sont pas identiques aux originaux);
- des documents réalisés de façon régulière et parce que la personne y était obligée (pas des document préparés à des fins intéressées).

Il arrive souvent que les systèmes informatiques ne puissent pas satisfaire à ces normes apparemment simples. Comme nous l'avons indiqué précédemment, les ordinateurs sont impersonnels. Les fichiers sont souvent tenus à jour et manipulés par une personne qui ne sait rien de leur création. Il est possible de les récupérer de nombreuses années après la survenance des événements enregistrés. Les fichiers d'un système informatique peuvent être un amalgame d'informations créées au sein d'une organisation et de renseignements provenant d'autres systèmes informatiques échappant au contrôle, à la connaissance ou à la responsabilité d'une seule personne. Les faits stockés dans un ordinateur peuvent faire partie d'un système logiciel servant à les manipuler, comme dans le cas d'un tableur pouvant produire d'innombrables variations à partir des mêmes données. Il est clair que la loi sur la preuve devra évaluer pour tenir compte de l'archivage des documents électroniques.

La Conférence sur l'uniformisation des lois au Canada a récemment approuvé une ébauche de la *Loi sur la preuve électronique*. Ce document traite de nombreuses questions concernant la preuve, comme l'authentification, la règle de la meilleure preuve et les procédures courantes. Pour obtenir de plus amples renseignements, consultez le site http://www.law.ualberta.ca/alri/ulc/current/eueaa.htm.

En vertu du projet de loi C-54 du gouvernement fédéral, traité ailleurs dans le présent rapport, un document électronique pourrait satisfaire aux exigences des lois fédérales mentionnées en annexe qui exigent des copies. Le projet règle les questions relatives aux documents originaux en considérant que les documents électroniques sont satisfaisants si «le document électronique comporte une signature électronique sécurisée, ajoutée lors de la production originale du document électronique dans sa forme définitive, pouvant être utilisée pour établir que le document électronique n'a pas été modifié depuis». Cet énoncé peut prêter à diverses interprétations, y compris ce qu'on entend par «production originale» et «forme définitive», avec toutes les versions intermédiaires possibles.

Le projet de loi C-54 traite des questions relatives à l'authentification et à la meilleure preuve en ces termes :

> «31.2 (1) Tout document électronique satisfait à la règle de la meilleure preuve dans les cas suivants :
> a) la fiabilité du système d'archivage électronique au moyen duquel ou dans lequel le document est enregistré ou mis en mémoire est démontrée;
> b) une présomption établie en vertu de l'article 31.4 s'applique.
> (2) Malgré le paragraphe (1), le document électronique sous forme de sortie imprimée satisfait à la règle de la meilleure preuve si la sortie imprimée a de toute évidence ou régulièrement été utilisée comme document relatant l'information enregistrée ou mise en mémoire.
> 31.3 Pour l'application du paragraphe 31.2(1), le système d'archivage électronique au moyen duquel ou dans lequel un document électronique est enregistré ou mis en mémoire est réputé fiable, sauf preuve contraire, si, selon le cas :
> a) la preuve permet de conclure qu'à l'époque en cause, le système informatique ou autre dispositif semblable fonctionnait bien, ou, dans le cas contraire, son mauvais fonctionnement n'a pas compromis l'intégrité des documents électroniques, et qu'il n'existe aucun motif raisonnable de mettre en doute la fiabilité du système d'archivage électronique;
> b) il est établi que le document électronique présenté en preuve par une partie a été enregistré ou mis en mémoire par une partie adverse;
> c) il est établi que le document électronique a été enregistré ou mis en mémoire dans le cours ordinaire des affaires par une personne qui n'est pas partie à l'instance et qui ne l'a pas enregistré ni ne l'a mis en mémoire sous l'autorité de la partie qui cherche à le présenter en preuve.
> 31.4 Le gouverneur en conseil peut prendre des règlements établissant des présomptions relativement aux documents électroniques portant une signature électronique sécurisée, notamment des règlements visant :
> a) l'association de signatures électroniques sécurisées à des personnes;
> b) l'intégrité de l'information contenue dans un document électronique portant une signature électronique sécurisée;
> c) la manière de prouver toute question visée aux alinéas a) ou b).
> 31.5 Afin de déterminer si, pour l'application de toute règle de droit, un document électronique est admissible, il peut être présenté un élément de preuve relatif à toute norme, toute procédure, tout usage ou toute pratique touchant la manière

d'enregistrer ou de mettre en mémoire un document électronique, eu égard au type de commerce ou d'entreprise qui a utilisé, enregistré ou mis en mémoire le document électronique ainsi qu'à la nature et à l'objet du document.»

La juxtaposition du droit de la preuve et des ordinateurs soulève de nombreuses questions. Au fur et à mesure que les institutions gouvernementales confieront leurs documents aux ordinateurs, les questions traitées dans la présente section seront résolues. Entre-temps, la conception du SDÉ tient compte de ces questions, y compris celles qui sont sans réponse.

10. Quelle sera l'incidence du SDÉ sur les renseignements confidentiels déposés auprès de l'Office et de la Commission?

On peut fournir des renseignements commerciaux confidentiels à l'Office et à la Commission (comme ceux indiqués à l'article 16.1 de la *Loi sur l'Office national de l'énergie* ou à la partie VII de la *Loi sur la Commission de l'énergie de l'Ontario*, 1998). D'autres principes d'application générale, comme les obligations fiduciaires, peuvent également s'appliquer comme ils le font présentement. On ne prévoit pas que le SDÉ proposé aura une incidence sur la confidentialité. Les différences entre le système de documents papier existant et le SDÉ proposé sont principalement liées à la sécurité informatique par rapport à la sécurité existante, traitée ailleurs dans le présent rapport.

11. Quelle sera l'incidence du SDÉ sur la justice naturelle et l'équité de la procédure?

Les concepts de justice naturelle et d'équité de la procédure permettent de faire en sorte que les parties concernées connaissent la cause qui sera entendue et qu'elles puissent présenter leurs preuves et leurs arguments devant un tribunal impartial. Les normes de procédure particulières qui permettront de s'en assurer dépendent de nombreux facteurs, dont le type de tribunal et les conséquences de la décision. Les tribunaux ont statué que les concepts d'équité et de justice naturelle ne devaient pas nécessairement s'appliquer à chaque tribunal, mais plutôt selon les circonstances. Les différents types de tribunaux accomplissent différentes choses, de la détermination des droits individuels, d'une part, aux recommandations de principe de portée générale, d'autre part. On applique des règles de procédure moins strictes aux questions de principe. On a rédigé de nombreux traités volumineux sur ces concepts qui ne feront pas l'objet d'une définition plus approfondie dans le présent rapport.

Dans la mesure où le SDÉ correspond simplement à l'automatisation de la création, de la transmission, de la mise en mémoire et de la récupération de documents, il ne devrait avoir aucun effet sur les normes de procédure. Autrement dit, l'Office et la Commission continueront de tenir des audiences, de prendre des décisions, etc. Cependant, plusieurs aspects du SDÉ méritent des remarques particulières.

La première a trait à la question de l'équité envers les personnes, les petits groupes d'intervenants et ceux qui n'utilisent pas les ordinateurs présentement. Est-ce qu'un système reposant sur l'utilisation de l'informatique aura pour effet d'exclure des gens? Non.

La plupart des participants aux instances de l'Office et de la Commission sont représentés par des avocats qui ont accès aux ordinateurs. Un sondage mené auprès d'eux indique qu'ils utilisent différents types de systèmes informatiques. On a procédé au sondage au début des étapes de planification du SDÉ et il ferait certainement état d'un perfectionnement technique encore plus poussé aujourd'hui. Il y a aussi des intervenants non représentés, principalement préoccupés par des questions comme la construction sur leur propriété, et un plus grand nombre de personnes non représentées qui n'interviennent pas, mais qui présentent leurs points de vue en transmettant leurs commentaires par la poste.

Quiconque participe aux audiences en vertu du présent système doit être en mesure de lire l'une ou l'autre des langues officielles, de respecter les règles de l'Office et de la Commission et de communiquer par courrier ou par télécopieur ou d'assister en personne. Ces exigences ne sont pas perçues comme étant injustes. Le système proposé crée peu de changements à cet égard. Il est possible de convertir les documents papier sous une forme électronique compatible avec les normes de l'Office et de la Commission. Même si une personne ne possède qu'un stylo et du papier ou une machine à écrire, elle peut soumettre un document papier et le SDÉ peut mettre en mémoire une version numérique de ce dernier.

Réciproquement, pour aider le public à obtenir des documents stockés dans le système, on mettra des ordinateurs à sa disposition pour permettre la recherche en ligne. Est-ce que cela exclut les citoyens qui ne savent pas comment chercher des documents dans un système informatique? Le régime actuel sert toujours de base de référence à la comparaison. Les gens savent-ils comment trouver des documents dans le système actuel? Ils doivent prendre le temps de comprendre les règles, le processus et les documents papier. Les rapports d'étape et les études sur le SDÉ laissent entendre que la récupération des documents sera grandement améliorée avec le système proposé. De plus, le tribunal a le pouvoir de réglementer ses procédures et, en particulier, d'exiger que l'information soit déposée avec des index, des résumés, des renvois et autres techniques pouvant réduire la complexité des causes même les plus considérables.

Il convient aussi de se demander si l'utilisation de l'informatique éloignera encore plus l'Office et la Commission du public. Les ordinateurs ne sont désormais plus des outils spécialisés conçus pour les experts — pas à une époque où les enfants des écoles publiques utilisent Internet en classe, où les compagnies de téléphone et de câblodistribution font en sorte que le courrier électronique soit aussi répandu que le téléphone et la télévision, et où de nombreux organismes gouvernementaux annoncent leurs sites Web. Le SDÉ proposé rapprochera l'Office et la Commission de la population à de nombreux égards : l'accès à l'information s'améliorera, grâce non seulement à la recherche automatisée, mais aussi à l'uniformisation accrue du dépôt des documents et du marquage des mots clés. Le SDÉ peut également fournir aux

personnes handicapées des formes d'accès qui ne leur sont pas offertes présentement, y compris l'informatique hors site, l'affichage à gros caractères, le braille et la synthèse vocale. Le SDÉ rapprochera l'Office et la Commission des participants situés en région éloignée.

En fait, l'accès électronique peut ouvrir les portes de l'Office et de la Commission à de nouveaux publics. Un dépôt central de documents électroniques peut fournir de l'information publique à toute personne reliée à Internet. Les gens ont toujours pu consulter les documents publics, mais seulement aux bureaux de l'Office et de la Commission. L'information accessible et consultable instantanément est un nouveau phénomène, peut-être même une nouvelle catégorie d'information publique.

Il se peut qu'il faille revoir les règles actuelles de pratique et de procédure pour les adapter au SDÉ. Elles sont présentement conçues pour un monde de documents papier. Il faudra réexaminer, par exemple, des mots comme «original» et «copie» dans le contexte du dépôt électronique. Les règles, les directives et les procédures devront évidemment tenir compte des droits et des besoins des participants qui ne possèdent pas d'ordinateur ou qui ont de la difficulté à les utiliser. L'Office et la Commission fourniront un accès à toute personne, selon les besoins, par le biais des ordinateurs ou des documents papier classiques. Ceux qui ne possèdent pas d'ordinateur ne seront pas laissés pour compte.

La question des avis est un aspect qui mérite une attention particulière. La justice naturelle et l'équité de la procédure exigent que les parties éventuelles soient averties de la tenue des audiences de l'Office et de la Commission. Le défaut de fournir un avis raisonnable peut invalider une décision. Il n'est pas nécessaire de remettre en main propre un avis rédigé sur papier (consultez également la section traitant, de façon générale, de la signification des documents). Au contraire, comme il y a énormément de gens concernés, l'Office et la Commission publient habituellement leurs avis d'audience dans les journaux. Aucun tribunal canadien n'a statué sur l'utilisation d'un site Internet ou du courrier électronique pour avertir le public de la tenue des audiences. Par analogie avec des décisions déjà rendues, cependant, il est probable qu'un tribunal cherchera à savoir si les moyens électroniques utilisés pour signifier les avis sont raisonnables dans les circonstances. Jusqu'à ce que l'utilisation d'Internet et de la technologie informatique devienne aussi courante que la lecture des quotidiens, toutefois, l'Office et la Commission continueront d'employer les moyens classiques, outre les moyens électroniques, pour aviser le public.

12. Comment les documents seront-ils signifiés avec le SDÉ?

Aujourd'hui, on crée la plupart des documents de façon électronique au moyen de logiciels de traitement de textes ou d'autres applications comme les tableurs et les logiciels de courrier électronique. Ils sont ensuite imprimés, déposés et signifiés sous forme de papier aux parties à l'audience. Certains participants peuvent alors numériser le document afin d'en faciliter la mise en mémoire, la recherche et la récupération sous

forme électronique. Le dépôt central des documents du SDÉ peut éliminer certaines de ces conversions et permettre l'extraction des documents du système, au besoin.

Dans un système papier, les documents sont non seulement déposés auprès du tribunal, mais également signifiés aux parties intéressées. Le dépôt et la signification permettent de s'assurer que les parties savent que des documents existent et qu'elles y ont accès. De plus, elles ne peuvent pas prétendre qu'elles ignoraient l'existence des documents déposés. Voilà un exemple où tous les documents sont toujours remis à toutes les parties, peu importe leurs intérêts particuliers dans l'instance en question.

Dans un système électronique, l'automatisation permet différents types de signification ou son élimination complète. Les parties peuvent passer l'information au crible en fonction de leurs propres intérêts. Elles peuvent recevoir des documents par courrier électronique. Ou, plutôt que de recevoir des documents complets, elles peuvent simplement être avisées que certains documents ont été déposés. Elles pourraient alors extraire des documents du dépôt central, au besoin. Elles pourraient encore se passer complètement de la signification et vérifier la présence de nouveaux documents dans le dépôt central soit manuellement, soit au moyen d'un logiciel automatique à la recherche des mises à jour périodiques.

Aucun tribunal canadien n'a statué sur la légalité de la signification des documents numériques ou l'élimination complète de la signification au profit de l'extraction des documents. Compte tenu de la jurisprudence relative aux technologies, comme le télécopieur et le télégraphe, un tribunal aurait tendance à examiner la technologie en question et les circonstances. De toute façon, l'Office et la Commission ont le pouvoir de modifier leurs règles de procédure, ils ne sont pas liés par les exigences procédurales des tribunaux et ils ont prescrit leur propres règles en matière de dépôt et de signification (Règles de pratique et de procédure de l'Office national de l'énergie, 1995, DORS/95-208, art. 8 et 9, Commission de l'énergie de l'Ontario - Règles de pratique et de procédure, février 1997, art. 11 et 20).

Comme dans le cas du système de documents papier actuel, si les parties connaissent tous les documents déposés et qu'elles y ont accès, compte tenu de dispositifs de protection appropriés, comme les messages d'accusé de réception, il serait alors possible d'atteindre les objectifs de la signification des documents par voie électronique. Bien qu'aucune spécification finale n'ait été précisée, le SDÉ est conçu de façon à réaliser ces objectifs.

13. L'Office et la Commission ont-ils tenu compte de l'incidence du SDÉ sur la pratique du droit?

Voici des déclarations d'avocats publiées dans *La revue des juristes de l'Ontario*, en février 1997, par le Barreau du Haut-Canada, qui régit la pratique du droit en Ontario :

> «La pratique du droit est très conservatrice.... nous ne serons pas les premiers à vouloir déterminer l'admissibilité d'un document électronique en cour.»

> «C'est comme retourner vers le passé, mais je ne me sens pas à l'aise face à ce monde entièrement électronique si ma carrière doit reposer sur le fait que la télécopie que j'ai envoyée à partir de mon ordinateur a été effectivement transmise.»

Les questions relatives à la pratique du droit comprennent la nécessité de déterminer si les instructions des clients doivent être signées sur papier. Des directives transmises par courrier électronique pourraient-elles suffire? Le cas échéant, pendant combien de temps faudrait-il conserver les vieux messages électroniques? Certains avocats peuvent croire que seuls les documents papier peuvent les protéger contre les réclamations pour faute professionnelle et qu'il faut conserver tous les documents à perpétuité. Ce genre de questions entre avocats et clients n'aboutît généralement pas devant un tribunal de réglementation. Néanmoins, des avocats comme ceux cités ci-dessus peuvent croire qu'ils doivent échanger du papier et non des électrons par excès de prudence.

D'ici la mise en oeuvre complète du SDÉ, on prévoit que les avocats utiliseront les ordinateurs dans d'autres secteurs de leurs activités et qu'ils auront adopté des politiques en matière de documents électroniques et d'archivage. Entre-temps, toute mise en oeuvre du SDÉ devra tenir compte dans une certaine mesure des responsabilités professionnelles des avocats par rapport à la tenue des dossiers.

14. Cela signifie-t-il que l'Office et la Commission ont répondu à toutes les questions au sujet du SDÉ?

Non. Le SDÉ est nouveau. D'ici à ce qu'il soit mis en oeuvre et testé, il y aura naturellement des questions et des problèmes à résoudre. Comme nous l'avons indiqué au début, de nombreuses questions seront résolues lorsque la nouvelle technologie sera mieux connue au fil du temps. Si des questions demeurent sans réponse, l'Office et la Commission accueilleront volontiers les commentaires et les suggestions.

15. Annexe A : Autres organismes et gouvernements

Bien que le SDÉ et les questions qui en découlent soient nouveaux dans la réglementation de l'énergie au Canada, l'Office et la Commission ne sont pas seuls. D'autres organismes et gouvernements passent également des documents papier aux systèmes électroniques.

Exemples du gouvernement fédéral canadien

Le gouvernement du Canada a mis en place de trop nombreux programmes électroniques pour pouvoir tous les énumérer ici (on peut en consulter la liste à http://www.gc.ca/programs/pgrind_f.html). Elle comprend :

AGENCE CANADIENNE D'ÉVALUATION ENVIRONNEMENTALE (ACÉE)

L'Agence canadienne d'évaluation environnementale, en vertu de l'article 55 de la *Loi canadienne sur l'évaluation environnementale,* tient un registre public. Ce dernier a pour objet de faciliter l'accès du public aux documents concernant les évaluations environnementales et d'assurer un accès convenable à la population. Le registre public comprend l'Index fédéral des évaluations environnementales, une liste de documents du ministère et des documents.

OFFICE DE LA PROPRIÉTÉ INTELLECTUELLE DU CANADA (OPIC)

L'Office de la propriété intellectuelle du Canada permet les recherches en ligne dans la Base de données sur les brevets canadiens. Voici la description qu'en donne le site Internet :

> «La Base de données met à votre disposition la description et la reproduction des documents de brevets déposés au cours des soixante-quinze dernières années. Vous pouvez rechercher, interroger et étudier plus de 1 400 000 documents de brevets.»

L'OPIC offre également la Base de données sur les marques de commerce canadiennes, qui est décrite ainsi :

> «vous offre maintenant accès à la Base de données sur les marques de commerce canadiennes. L'information qui se trouve dans cette base de données peut inclure des dessins de marques de commerce, les marchandises et services, les noms des propriétaires et plus.»

SIGNATURES NUMÉRIQUES

Le gouvernement fédéral utilise déjà la technologie des signatures numériques, comme dans le cas d'une nouvelle application décrite en ces termes :

> Le 5 juin 1998, M. Mah Bow Tan, ministre des communications de Singapour, a utilisé une signature numérique pour signer un protocole d'entente entre son pays, le Canada et l'État de la Pennsylvanie. La signature a eu lieu lors d'une réunion de l'Organisation de coopération économique Asie-Pacifique sur l'industrie des télécommunications et de l'information. M. John Manley, ministre canadien de l'Industrie, et M. Tom Ridge, gouverneur de la Pennsylvanie, qui n'étaient pas présents à la réunion, avaient signé le document au préalable au moyen de la technologie des clés privées. Des représentants ont remis les documents ainsi signés au ministre Mah selon le cérémonial d'usage durant la réunion. Il a ensuite inséré une carte à puce contenant sa signature dans le lecteur et tapé son mot de passe pour «signer» le document. Les trois signatures ont ensuite fait l'objet d'une authentification pour créer un document officiel. Ce premier document gouvernemental international signé de façon numérique crée un consortium d'apprentissage mondial entre les deux pays et l'État pour promouvoir l'utilisation de la technologie des télécommunications et de l'information en éducation par l'intermédiaire d'un site Web commun. (http://www.tas.gov.sq)

Exemples de l'Ontario

En Ontario, parmi les premiers exemples d'utilisation des systèmes électroniques, mentionnons l'enregistrement des sûretés mobilières, l'enregistrement des noms commerciaux, l'enregistrement des titres fonciers, les procédures régissant les procès civils et les dépôts auprès de la Commission des valeurs mobilières.

MINISTÈRE DU PROCUREUR GÉNÉRAL DE L'ONTARIO

Un projet pilote autorisé en vertu de la *Loi sur les tribunaux judiciaires* (Règlement de l'Ontario 223-97) permet aux avocats de déposer un nombre limité de documents au civil par voie électronique. Le dépôt électronique fait partie d'un projet plus important de gestion des causes civiles au moyen d'un logiciel privé appelé Sustain permettant d'entrer les réclamations, de planifier les causes et de produire des rapports statistiques. Seuls les cabinets d'avocats et les services juridiques ayant reçu une formation sur l'utilisation du logiciel prescrit peuvent y participer. Dans le cadre du projet pilote, un avocat utilise le logiciel client Sustain pour créer, puis envoyer par voie électronique un fichier de traitement de texte d'une page au greffe du tribunal. Le logiciel vérifie le formulaire, débite les droits de dépôt directement du compte de l'avocat, émet un numéro de référence et envoie un reçu à l'avocat. Il est possible de signifier des documents entre les procureurs participants par l'intermédiaire du système informatique. Les formulaires prescrits ne nécessitent pas de signature, bien que l'avocat doive conserver une preuve signée de la signification. L'accès public aux documents déposés sera initialement offert par le biais des terminaux du tribunal et, ultérieurement, par accès à distance et on produira également des copies papier au besoin. Les plans à long terme, qui ne font pas partie du projet pilote, comprennent le dépôt des motions et des dossiers des procès en plus des documents simples d'une page.

Le système Sustain, contrairement au SDÉ, utilise des logiciels et des formats de données exclusifs. Un consortium de sociétés, dont Microsoft, fait la promotion du logiciel comme moyen d'établir des liens électroniques entre les avocats et les tribunaux. Le projet ministériel est également associé à un processus distinct de gestion des tribunaux administratifs.

MINISTÈRE DE LA CONSOMMATION ET DU COMMERCE

En partenariat avec une société privée, Teranet, le ministère de la Consommation et du Commerce a mis au point un système électronique d'actes translatifs de propriété. Le ministère possède également un système électronique permettant de déposer les enregistrements de sûretés mobilières et un système pour l'enregistrement des noms commerciaux. Plus de 90 % des enregistrements de sûretés mobilières et 30 % des enregistrements de noms commerciaux en Ontario sont déposés par voie électronique. Ces systèmes utilisent des logiciels et des formats de données exclusifs. Dans la plupart des cas, seules les personnes désignées peuvent y participer. En vertu des règlements régissant ces systèmes, il n'est pas nécessaire que les documents soient signés. Contrairement au SDÉ, ces registres ne sont pas principalement destinés à la gestion des documents aux fins d'audiences et de décisions.

Exemple pancanadien

AUTORITÉS CANADIENNES DE RÉGLEMENTATION DES VALEURS MOBILIÈRES

Les autorités canadiennes de réglementation des valeurs mobilières ont adopté un système de dépôt électronique, le Système électronique de données, d'analyse et de recherche (SEDAR), qui a été mis au point afin de :

> «faciliter le dépôt électronique de l'information reliée à la réglementation des valeurs mobilières (prospectus, documents d'information continue, etc.) et le paiement des droits de dépôt aux autorités canadiennes de réglementation des valeurs mobilières;
>
> faciliter la diffusion publique de l'information reliée à la réglementation des valeurs mobilières rassemblée dans le cours du processus de dépôt;
>
> faciliter les communications électroniques (courrier électronique, etc.) entre les déposants par voie électronique, les agents de dépôt et les autorités en valeurs mobilières.»
> (Manuel du déposant SEDAR)

À moins de circonstances exceptionnelles, tous les documents déposés doivent maintenant être présentés sous forme électronique. Contrairement au SDÉ proposé, SEDAR n'utilise pas le langage standard généralisé de balisage (LSGB). Tous les documents SEDAR doivent être réalisés au moyen de l'un des trois formats exclusifs suivants : WordPerfect, Microsoft Word ou Adobe PDF.

Exemples des États-Unis

RULENET

RuleNet, une expérience innovatrice menée par la Nuclear Regulatory Commission (NRC) des États-Unis, était un forum électronique d'élaboration de règlements sur Internet. L'expérience visait à faire participer le public à la préparation de règles fondées sur le rendement en matière de protection contre l'incendie. Toute personne pourvue d'un navigateur Web pouvait observer, formuler des commentaires et accéder à des documents connexes. (http://nssc.llnl.gov/RuleNet/Help/Info.html)

FEDERAL COMMUNICATIONS COMMISSION (FCC)

En avril 1997, la FCC a lancé son initiative de dépôt électronique au moyen d'un avis de projet de réglementation (FCC 97-113) :

> Dans cet avis de projet de réglementation (avis), nous proposons de permettre aux parties de déposer leurs commentaires par voie électronique dans le cadre de toutes les instances (avis et commentaires) informelles de la FCC relatives à l'élaboration des règlements en vertu de l'article 553 du *Administrative Procedure Act*, sauf en ce qui a trait aux procédures d'attribution en matière de radiodiffusion. Ces dépôts électroniques se verront accorder un traitement et une importance identiques à ceux des commentaires déposés au moyen de documents papier. Nous avons conclu provisoirement que cette initiative permettra au public de communiquer ses points de vue beaucoup plus facilement à la Commission et d'analyser les commentaires que d'autres ont déposés. Nous croyons que le dépôt électronique permettra également à la Commission d'améliorer l'efficacité de ses propres processus au bénéfice du public.

AUTRES ORGANISMES UTILISANT LE LSGB

Voici une liste provenant de la page Web du LSGB (http://www.oasis-open.org/cover/ de novembre 1998) présentant les projets LSGB en cours dans les secteurs publics et privés :

- Office of Scientific and Technical Information (OSTI) du Department of Energy (DOE) des États Unis;

- IRS (Internal Revenue Service des États-Unis);

- National Library of Medicine (NLM);

- Library of Congress - Encoded Archival Description (EAD) (description des archives codées) - Finding Aid Pilot Project (projet pilote sur les instruments de recherche);

- Automotive and Truck Standard SAE J2008 (et T2008);

- Base de données SEC EDGAR;

- IETM (Interactive Electronic Technical Manuals) (manuels techniques électroniques interactifs);

- TCIF/IPI (Telecommunications Industry Forum Information Products Interchange) (échange réciproque de produits d'information sur les forums de l'industrie des télécommunications);

- Electronic Component Information Exchange (ECIX) (échange d'information sur les composants électroniques) - Pinnacles Component Information Standard (PCIS) (norme d'information sur les composants Pinnacles);

- Définitions des types de documents de l'Association du transport aérien;

- Railroad Industry Forum: Electronic Parts Catalog Exchange Standard (EPCES) (forum de l'industrie ferroviaire : norme d'échange des catalogues de pièces électroniques);

- CALS : Soutien continu des acquisitions et de leurs cycles de vie (anciennement : Groupe de travail - Acquisition et soutien logistique assisté par ordinateur; récemment : Commerce à la vitesse de la lumière);

- USAF SGML Repository (dépôt central des documents en LSGB des forces aériennes américaines);

- Norme militaire 2167A : FOSI et définitions des types de documents relatifs à la norme militaire 2167A;

- Documents MIL-M-28001B en LSGB(site des forces navales);

- Army SGML Registry and Library (ASRL) (registre et bibliothèque LSGB de l'armée);

- Technologie de recherche d'information du gouvernement - GIFT (Canada).

16. Annexe B : Autres documents à consulter

Aspects of Public Policy Regarding Crown Copyright in the Digital Age, W.T. Stanbury, 10 *Intellectual Property Journal* 131, mai 1996

Copyright and Confidential Information Law of Canada, G. F. Henderson édit., 1995, Carswell

Copyright and the State in Canada and the United States, David Vaver, 10 *Intellectual Property Reports* 187, mai 1996

Copyright in Legal Documents, David Vaver, 1993 *Osgoode Hall Law Journal*, vol. 31, n° 4, p. 662

Crown Copyright In Canada: A Legacy Of Confusion, Barry Torno, 1981, ministre des Approvisionnements et Services

Essentials of EDI Law, Peter Jones, Conseil canadien de l'échange électronique de données, 1992

The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet, Stephen M. Johnson, *Administrative Law Review*, 50:2, printemps 1998, pp. 277 et suivantes;

Management of Recorded Information, Directive 7-5-8, juin 1992, Conseil de gestion du gouvernement (Ontario)

Microfilms et images électroniques - preuve documentaire, CAN/ONGC - 72.11-93, Office des normes générales du Canada

La revue des juristes de l'Ontario, janvier/février 1997, vol. 1, n° 1, Barreau du Haut-Canada

Open Access Same-Time Information System, 18 CFR Part 37, 24 avril 1996, Federal Energy Regulatory Commission (FERC)

Policy, Practice and Who Gets to Own the Crown's Jewels: The Ownership of Intellectual Property in Crown Contracts, Martin P. J. Kratz, 10 C.I.P.R. 613

Practitioner's Guide to Electronic Filing in Utah Courts, 27 avril 1995, Utah Administrative Office of the Courts

Recorded Information Fact Sheet # 6 on Electronic Document Filing Fundamentals, Archives publiques de l'Ontario

Rapport du Comité directeur de la stratégie - sécurité de la technologie de l'information au Conseil du renouveau administratif, juin 1995 (http://www.cse.dnd.ca/GOCITSTRATEGY/).

Circulaire d'information de Revenu Canada, 78-10R2SR, 10 février 1995

SEDAR (Système électronique de données, d'analyse et de recherche), Commission des valeurs mobilières de l'Ontario (CVMO), bulletin du 15 novembre 1996, volume 19, n° 46, supplément du SEDAR

SGML Handbook, Charles F. Goldfarb, 1990, Oxford University Press

Normes relatives à la façon de rédiger, de distribuer et de citer les jugements canadiens sous forme électronique, mai 1996, Comité consultatif sur l'utilisation de l'informatique par les juges du Conseil canadien de la magistrature

Étude des questions de droit entourant la sécurité des renseignements électroniques, Stratégie pour la sécurité des technologies de l'information - groupe de travail sur les questions de droit, juin 1995, Conseil du Trésor du Canada

Sustaining Dialog, ministère du Procureur général, bulletin trimestriel relatif au projet Sustain de dépôt des documents juridiques

Who Owns Copyright in Law Reports? Gérard Snow, 64 C.P.R. (2d) 49

17. Annexe C : Glossaire

Authentification : légitimation des personnes et des machines.

Octet : huit chiffres binaires (bits, c'est-à-dire des uns et des zéros) pouvant représenter 256 nombres ou caractères (entre 0 et 255, représentés par 00000000 à 11111111); unité fondamentale de transmission ou de stockage de l'information dans un ordinateur.

CGM : Computer graphics metafile, un format de fichiers d'image.

Cryptographie : science de la sécurisation des messages.

Signature numérique : processus informatique conçu aux mêmes fins que la signature manuscrite; moyen électronique d'associer une personne à un document; résultat de l'utilisation de processus technologiques particuliers pour authentifier un document.

Définition de type de document : structure de document prescrite exprimée en langage LSGB (q.v.); la structure de tous les documents déposés en vertu du SDÉ doit être conforme à la définition du type de document prescrite.

Courrier électronique : courrier envoyé sous forme d'une chaîne d'octets (q.v.) d'un ordinateur à un autre par l'intermédiaire d'Internet (q.v.) ou d'un réseau privé; peut désigner le système ou les messages eux-mêmes.

SDÉ : Système de dépôt électronique, projet conjoint de l'Office national de l'énergie et de la Commission de l'énergie de l'Ontario visant à remplacer les processus reposant sur des documents papier par des systèmes numériques pour faciliter la création, l'échange, l'utilisation et la réutilisation de l'information réglementaire.

HTML : Hypertext Markup Language, sert à créer des pages Web sur Internet avec des liens, appelés hyperliens, vers d'autres pages Web; HTML est une définition de type de document (q.v.) décrite par le métalangage LSGB (q.v.).

Internet : réseau de réseaux informatiques utilisant un protocole de communication convenu, appelé Transmission Control Protocol/Internet Protocol (TCP/IP), qui facilite les services courants comme le courrier électronique, les pages Web et les transferts de fichiers.

JPEG : format de fichiers d'image provenant du Groupe mixte d'experts en photographie, également appelé fichiers JPG, permettant de stocker et de transmettre des photographies dans un système informatique.

MPEG : format de compression vidéo numérique provenant du Groupe d'experts pour le codage d'images animées permettant de stocker et de transmettre des films dans un système informatique.

PDF : Portable Document Format, format de fichiers de document exclusif de Adobe Systems Incorporated.

LSGB : langage standard généralisé de balisage, métalangage utilisé pour décrire des types de documents, comme HTML et XML (q.v.); sépare le contenu et la structure de la mise en forme et de l'aspect.

XML : Extensible Markup Language sous-ensemble du LSGB (q.v.); on prévoit qu'il sera le format des documents de prochaine génération sur le Web (q.v).

World Wide Web : documents liés stockés dans des ordinateurs branchés à Internet (q.v.), également appelé le Web, d'où l'expression page Web désignant un seul document; les adresses des documents commencent fréquemment par www, soit l'abréviation de World Wide Web, comme dans www.neb.gc.ca ou www.oeb.gov.on.ca.